Question reference	Section number and name	Topic	ARPANSA Comment, Issue and/or Question and ANSTO's Response
PSA.1.	1. Introduction	The report documents the Probabilistic Safety Assessment (PSA) of the Replacement Research Reactor (RRR). The PSA is basically a Level 1, and shows the core damage frequency (CDF). There are some Level 3 considerations also that indicate the frequency and consequences of a few sequences.	The text makes no mention of Level 2 PSA considerations, and the availability and performance of the containment is not considered.
			Response: Since the CDF was shown to be below the lowest frequency of the ARPANSA safety objective (*ie* 10^{-6} pa), no level II or III analysis was performed for these plant damage states. For other events where the frequency was above this objective, conservative assumptions were made about the containment and related issues in order to obtain a conservative estimates of the dose without the need for detailed phenomenology of both the fuel/target melt or damage and containment response. This demonstrates that the RRR will meet the safety objectives. Refer to Section 7.1 of the PSA.

Question reference	Section number and name	Topic	ARPANSA Comment, Issue and/or Question and ANSTO's Response
PSA.2.	1.1.2 How does the PSA fit with the Safety Analysis.	The Safety Analysis is in Ch.16 of the PSAR. It considers a range of Postulated Initiating Events (PIES). In the PSAR a number of PIES are eliminated because their likelihood is low, because of plant design features that the PIE cannot credibly occur, or because the consequences are bounded by other PIEs. The events that remain are the Design Basis Events. The PSA attempts to determine all the possible combinations of how the plant could respond to initiating events, and also looks at beyond design basis accidents.	A key issue for both Ch.16 and the PSA is the process of screening out or eliminating PIES from further consideration. This is referred in many of the following comments on the PSA. It is noteworthy that beyond design basis accidents are not considered in detail in Ch.16. Information should be provided on how the comparison with the Siting Reference Accident (which is beyond design basis) has been carried out in the PSAR.
			Response: Chapter 16 deals with BDBA in Section 16.20. It should be noted that at this stage of the RRR project, there is no requirement to revisit the Siting Reference Accident other than to show that the assumptions made in it are valid. The PSA and Chapter 16 (see also Licence Application) show that the Siting Reference Accident was conservative for this design.
PSA.3.	1.1.3.2 Consequence.	The ARPANSA frequency-dose relationship (Table 2 of the RAPs) is reproduced as Table 1/1 of the PSA. The safety limits in Table 1/1 are taken as mandatory.	Table 1/1 allows for both deterministic and probabilistic approaches. Since the PSA is basically a Level 1 PSA, the approach to satisfying the frequency-dose relationship should be explained. Further justification is also required to show that the total frequency of each initiator has been used in the PSA analysis (*ie* that the frequency of initiators includes those that were screened out on the basis of being bounded by another).

Question reference	Section number and name	Topic	ARPANSA Comment, Issue and/or Question and ANSTO's Response
			Response: ARPANSA Regulatory Assessment Principle 29 permits deterministic approach to the demonstration of compliance with this table. PSA was used for the determination of end state frequencies whilst a deterministic approach was used with conservative assumptions for the determination of consequences. This complies with the Assessment Principles. The CDF was shown to be below the lowest frequency of the ARPANSA safety objective (ie 10^{-6} pa), and therefore no level II or III analyses were performed for these plant damage states. For other events where the frequency was above this objective, conservative assumptions were made about the containment and related issues in order to obtain a conservative estimates of the dose without the need for detailed phenomenology of both the fuel/target melt or damage and containment response. In general the event frequencies were chosen conservatively to bound a range of sequences.
PSA.4.	1.2 Objectives	A PSA is useful in quantifying risks from the operation of a nuclear reactor, and it can also be a useful design aid to estimate risk reduction benefits from changes. The PSA undertaken is full scope and covers internal events, external hazards, internal hazards and human factors. The PSA has been run in parallel with the design and has been an input into the design process.	The objectives of the PSA look satisfactory, and its input into the design process is a good practice. However, it is the detail modelling and assumptions that matter and this review raises a number of matters.
			Response: Comment noted.

Question reference	Section number and name	Topic	ARPANSA Comment, Issue and/or Question and ANSTO's Response
PSA.5.	1.3 Scope	The scope of the PSA is Level 1, with certain Level 3 considerations. There is no examination of Level 2 associated with the phenomenology of release, transport and deposition of radioactive materials within the containment. The consequence analysis that is undertaken shows that there is no design basis, or credible beyond design basis accident that exceeds 5 mSv to the critical group (at the 1.6km exclusion zone)	The PSA Level 3 considerations are not extensive since there is no detailed consideration of the Level 2 aspects, other than what was used in the Siting Reference Accident. Justification of the claims for no credible beyond design basis accident exceeding 5 mSv will be an important issue.
			Response: Comment noted. As indicated in response to Question PSA.3, the level II and III considerations were treated largely deterministically with conservative assumptions. This is a valid approach. The core damage frequency has been shown to be less than 10^{-6} pa, including external events with seismic to the 100,000 year return period. It is a valid and common practice to interpret plant damage states having frequency below 10^{-7} pa as "not credible" and not to analyse consequences when the summed frequency is below 10^{-6} pa. In the FSAR stage, the cut-offs, and screening assumptions will be reviewed and documented.

Question reference	Section number and name	Topic	ARPANSA Comment, Issue and/or Question and ANSTO's Response
PSA.6.	1.4 Method of Identification and Selection of Initiating Events	The Source and Event Analysis (SEA) method was used to identify and select the initiating events. The SEA method has a number of criteria ((a) to (e)), and a large list of failure mechanisms and initiating events is generated. A screening process is performed at each step to screen out events which make a negligible contribution to risk.	The screening out process using the SEA method is an important issue. Low frequency events screened out in an initial cut set may become important if the bottom line CDF values are as low as 10^{-7} to 10^{-8} per year. These low frequency events may be associated with Level 2 phenomenology that could increase the release and consequences.
			Response: It was recognised that early screening did remove events that were later shown not to be insignificant against the low value of CDF. For this reason, a reassessment was made and two events that had been screened out were "reinstated" — these were the large aircraft crash and military shelling events (Refer to Section 7.5 of PSA). Nevertheless, the screening will be reviewed again at the FSAR stage, and the screening assumptions documented. Consequence analysis is not required for such low frequency events, since compliance with the safety objective is already clear (because the frequency is below 10^{-6} pa).

Question reference	Section number and name	Topic	ARPANSA Comment, Issue and/or Question and ANSTO's Response
PSA.7.	1.5 Analysis Methods	The SAPHIRE (INEL) package was used for the RRR PSA. It follows the standard practice of developing an Interference Matrix, Fault Trees and Event Trees. An uncertainty analysis is also part of the SAPHIRE package and the results are presented as mean, 5% confidence levels and 95% confidence levels. Importance measures are also estimated using the Fussel-Vessely importance estimation.	The information on plant and human reliability comes from a number of sources, primarily the IAEA database and the HIFAR PSA. The applicability of this data to the RRR, particularly where there are novel designs is important. This is raised later in this review with respect to specific components and systems.
			Response: The RRRP is a reactor which is at the completion of the preliminary engineering phase. Whilst it is desirable to have plant specific data, it is not possible for a reactor that is at this stage. The estimates used are the best available at this stage and come from an internationally recognised source.
PSA.8.	1.6 Dependent Failures Analysis	Three types of dependent failures considered in the PSA: Functional dependencies between systems Dependencies or common causes between basic events Dynamic human interactions The functional dependencies are treated explicitly in the fault trees. Three types of common cause effects were modelled as human errors; design errors, maintenance errors and test, calibration and inspection errors	The approach to dependent failures is comprehensive. However, a major factor that emerges later in this review is the reliability given to humans in design, maintenance and testing. In regards to maintenance and inspection the justification for treating human reliability actions as independent should be explained.

Question reference	Section number and name	Topic	ARPANSA Comment, Issue and/or Question and ANSTO's Response
			Response: In all cases where they appear together, the maintenance and testing human error events appear in fault trees in OR gates (not AND gates). In such situations, the assumption of independence is the more conservative. This covers the case within systems. See also response to Question PSA.72. The assumption was made that there is no dependency of the human errors between or amongst systems. No credible scenario was identified for such dependencies because there are no similar HEM or HET events shared amongst systems. The maintenance and testing procedures will be drafted in a way that the hypothesis made in the PSA are valid.
PSA.9.	1.7 Safety Objectives	The Level 3 safety objectives in terms of dose and consequences are shown in Table 1/1 and Figure1/1. The Level 1 objectives are taken from the RAPs (principles 38 and 32.). with a CDF of 10^{-4} per year, and a reactor shutdown likelihood of 10^{-3} per demand.	The objectives are consistent with the ARPANSA RAPs principles. The approach used to provide compliance with the frequency-dose criteria requires further explanation. (SAME AS QUESTION 3)
			Response: See response to Question PSA.3
PSA.10.	2.1 Human Reliability Analysis	The THERP or Technique for Human Error Rate Prediction was used. It deals with errors of operation , test, maintenance or calibration. Unavailability continues until it is revealed by component not being operative or by other changes.	A major factor that emerges later in this review is the reliability given to humans in design, maintenance and testing. In regards to maintenance and inspection the justification for treating human reliability actions as independent should be given.
			Response: See response to Question PSA.8.

Question reference	Section number and name	Topic	ARPANSA Comment, Issue and/or Question and ANSTO's Response
PSA.11.	2.2.1 Common Cause Design Failure	Type D common cause failure represents a hidden design flaw in a set of identical components. There are a number of assumptions embedded in the estimation, such as design checks, design reviews, performance of a Failure Modes and Effects (FMEA) analysis. It is also assumed that the component all of the above is within a QA system. The scheme is shown in Fig. 2/1.	The reliability value (D CCF=$6.65*10^{-6}$) requires justification. The assumption that all checks and reviews are independent, that they are performed within a QA system, and the performance tests are realistic may not be true. The relevance of the ETRR.2 experience with key components such as "Flap valves" should be considered in this context.
			Response: Different design teams work on different systems. Design, manufacture and testing has and will take place in accordance with the INVAP QA system. Operational, maintenance and safety culture experience at ETRR-2 has been considered but is not indicative of operations at ANSTO. Comparison of the Human reliability method of estimating dependencies with other widely used methods show differences, but the comparison showed a similar overall effect on the systems. For example in the FSS, the adopted method corresponds to a beta factor of $3.3x10^{-5}/(4.0x10^{-5}+3.3x10^{-5})=0.45$.

Question reference	Section number and name	Topic	ARPANSA Comment, Issue and/or Question and ANSTO's Response
PSA.12.	2.2.2 Common Cause Maintenance Failure	Type M common cause failure represents an unrecognised failure caused during maintenance. There are a number of assumptions embedded in the estimation, such as a correct written maintenance procedure and that the tasks are supervised. The above tasks are also assumed to be within an operational QA system. The model is shown in Fig.2.2.	The reliability value M CCF=$1.1*10^{-3}$ requires justification. Reviews of abnormal occurrences or defects would indicate that maintenance errors are not infrequent, and are likely to effect common systems.
			Response: Maintenance will take place in accordance with the ANSTO QA system for the RRR. Typical HET and HEM values were estimated based on certain assumptions, which are considered to be valid for maintenance and testing work on safety related equipment in a nuclear reactor. Comparison of the Human reliability method of estimating dependencies with other methods showed differences, but overall the comparison showed a similar overall effect on the systems. For example in the compressed air supply system (Figure 4/9) the corresponding beta factor for the compressor failure is $1.1x10^{-3}/(2.4x10^{-2} + 1.1x10^{-3}) = 0.04$. For other cases the corresponding beta factor is much higher (> 0.5). This issue is clearly important and detailed analyses of the human error probabilities will be made during the detail engineering phase.

Question reference	Section number and name	Topic	ARPANSA Comment, Issue and/or Question and ANSTO's Response
PSA.13.	2.2.3 Common Cause Test Failure	Type T common cause failure represents an unrecognised failure caused during test or calibration. There are a number of assumptions embedded in the estimation, a written and correct test procedure exists and that the tests are supervised. The above tests are also assumed to be performed within an operational QA system. The model is shown in Fig 2.3.	The reliability value M-CCF=$1.1*10^{-3}$ requires justification. A whole range of maintenance tasks, from small to large may be done, and there may not be a need for a test recognised, or as often is the case there is no "realistic" test possible. It is possible that the tests may be carried out by the maintenance person, so there is not necessarily independence between maintenance tasks and tests.
			Response: Testing will take place in accordance with the ANSTO QA system for the RRR. See also response to Question PSA.12.
PSA.14.	2.3 Human Error Probability Data	Table 2/1 is based on the type D, M and T human failure probability estimates. The information is used for a range of human actions that fed directly into the event trees	See above comments on the need for justification of the D, M and T values derived.
			Response: Please see responses to Questions PSA.11, 12 and 13.
PSA.15.	3.1 Internal Initiating Events	The Source and Event Analysis (SEA) identifies all relevant potential radioactive sources, the barriers that contain them, and failure mechanisms that may cause failure.	The SEA has focussed on core damage since it is a Level 1 PSA. The treatment of the containment, or the electrical power supply availability should be further explained in that context.

Question reference	Section number and name	Topic	ARPANSA Comment, Issue and/or Question and ANSTO's Response
			Response: The statement that the SEA has focussed on core damage is incorrect. Core damage is typically the prime issue in PSA of nuclear reactors. However all sources of radioactive material that could potentially cause a dose to a member of the public were considered in the PSA. Please refer to Sections 3.1.1 and 3.1.2. Containment failure would not constitute an initiating event. Containment was considered in this PSA although not in a detailed way, rather in a simplified but conservative treatment (see also responses to Questions PSA.1 and 3). The PSA is more than Level I but does not claim to be Level II or Level III; rather, it is Level I with some Level III considerations. Loss of electric power is an initiator (B2) in the PSA.
PSA.16.	3.1.2 Barriers Failure Mechanism—Uncontrolled power increase.	A number of mechanisms are identified that involve erroneous withdrawal of control rods, extraction or ejection control rods, reflector heavy water ejection, inadvertent refill of the reflector tank, cold water injection and radioisotope production rigs. All of the mechanisms for uncontrolled power other than single control rod removal are screened out.	The screening out of these uncontrolled power increase mechanisms is sometimes based on judgements and not analysis. These judgements should be further justified.

Question reference	Section number and name	Topic	ARPANSA Comment, Issue and/or Question and ANSTO's Response
			Response: It is recognised that the validity of the screening out of some events will have to be confirmed by additional analysis. This will be included at the completion of the detail engineering phase. However, at this stage it is difficult to conceive failure modes where bank withdrawal of control rods could occur. (Refer to Chapter 5, Section 5.5.2.8 and Chapter 16, Sections 16.8.3.2 and 16.8.3.4 of PSAR and response to Question 8.72).
PSA.17.	3.1.2 Barriers Failure Mechanism—Uncontrolled power increase.	Two events are covered in the PSA, namely A1 single rod removal at start up, and A2 single rod removal at full power.	There is no consideration of operation at low power (say 100kw), when many of the First Reactor Protection System (FRPS) and Second Reactor Protection System (SRPS) parameters may not be enabled. This mode of operation should be modelled in the PSA, since it could be associated with a fresh fuel load
			Response: It should be noted that at low power a number of trips are available e.g. high neutron flux for both FRPS and SRPS and small reactor period for FRPS. For a fresh core load there are three start-up high-flux channels connected to the FRPS. Low power mode modelling will be performed and will be provided to ARPANSA.
PSA.18.	3.1.2 Barriers Failure Mechanism—Uncontrolled power increase.	Two events are covered in the PSA, namely A1 single rod removal at start up, and A2 single rod removal at full power.	The failure of the FSS in an earthquake should be considered. Justification should be provided that the shearing of the CRD anchorages within the CRR will not allow the base to deflect and distort preventing the five rods from dropping into the core

Question reference	Section number and name	Topic	ARPANSA Comment, Issue and/or Question and ANSTO's Response
			Response: Seismically induced failure of the individual control rods is included in the seismic model. However, it was assumed that the design of the CRD tables and anchors is such that multiple failure of rods to insert is not credible. Note that the consideration of an earthquake in conjunction with an A1 or A2 event is not credible. The failure of the FSS has been considered in the PSA in the form of the fragility curves used for earthquakes in excess of the SL-2 level. The FSS itself is a Seismic Class 1 (ref Chapter 2, Table 2.5/2 of PSAR) system that is designed to remain operational for earthquakes up to the SL-2 level. Ongoing work on the deflection of the CRD indicates that the system will remain operational (ie the CRs will drop into the core) for earthquakes in excess of the SL-2 level. This will be confirmed by the detailed seismic modelling and suitable tests will be devised.
PSA.19.	3.1.2 Barriers Failure Mechanism—Uncontrolled power increase.	Two events are covered in the PSA, namely A1 single rod removal at start up, and A2 single rod removal at full power.	Analysis needs to be provided to justify the screening out of the event "cold water injection into the core" The same comment is relevant to the screening out of temperature, degradation and refill effects within the Reflector Tank

Question reference	Section number and name	Topic	ARPANSA Comment, Issue and/or Question and ANSTO's Response
			Response: Two possible mechanisms have been identified for injection of cold water into the core: actuation of the EMWS and start up of the stand by PCS pump. The EMWS (See Chapter 6, Section 6.7 of the PSAR) is a passive system that injects water via the opening of a float valve in each branch when the pool water reaches a pre-set level. In the unlikely event that this valve opened during normal operation, the pressure inside the PCS piping would prevent injection of cold water from the EMWS storage tanks. During low power operation this event is bounded by the event of the start up of a PCS pump. Regarding the start up of the standby PCS pump, this is prevented by an interlock, both during full power and low power operation. Start up of a pump during full power and low power operations (worst possible case with sudden injection of 1000 m^3/h) results in a reactivity insertion of 0.5 $ (359 pcm), with a ramp of 3.9 $/s. This insertion results in a very mild transient bounded by the start up accident presented in Chapter 16, Sections 16.8.3.1 and 16.8.7.3 of the PSAR. Reflector tank refill is via a small peristaltic pump. This pump is not physically capable of injecting D_2O at a rate sufficient to cause a reactivity insertion with a significant ramp. Refer to Chapter 16, Section 16.8.5.1 of the PSAR.
PSA.20.	3.1.2 Barriers Failure Mechanism—Uncontrolled power increase.	Two events are covered in the PSA, namely A1 single rod removal at start up, and A2 single rod removal at full power.	Analysis needs to be provided to justify the screening out of the event "Inadvertent fast withdrawal of an irradiation can". The possibility of simultaneous ejection of more than one target (each worth 240 PCM), up to the maximum number of such rigs installed needs to be addressed.

Question reference	Section number and name	Topic	ARPANSA Comment, Issue and/or Question and ANSTO's Response
			Response: The same issue as Question PSA.19. These events were not screened out due to frequency consideration, but due to reactivity insertion rate consideration. Each can is only 40 pcm. The analysis was performed for 240 pcm (equivalent to the simultaneous withdrawal of 6 cans or one can with a large overload). Refer to Chapter 16, Section 16.8.3.6 of PSAR and Section 3.1.2 of the PSA. That said, it should be noted that the mechanical design of the pneumatic target load/unload controller prevents the simultaneous withdrawal of more than one target at any one time (see Chapter 11, Section 11.4.2 of the PSAR).
PSA.21.	3.1.2 Barriers Failure Mechanism—Uncontrolled reduction of heat removal.	A number of mechanisms that involve uncontrolled reduction of heat removal are described. These include core bypass, loss of power, primary pump failure, blockage in piping or heat exchanger, fuel channel blockage. Five scenarios are identified, B1, B2, B3, B4 and B5. To cover these loss of heat removal capacity.	A number of mechanisms for flow bypass are described, but only B1-pipe rupture and flap valve opening is in the event trees. The other mechanisms, such as flap valve failure, check valve failure should be considered since they may increase the frequency of B1
			Response: The text (Section 3.1.2 of the PSA) explains that no credible scenario for spurious opening of the flap valves could be postulated, yet it could not be argued that the frequency would be less than the frequency of rupture of a section of pipe. Therefore, flap valve spuriously opening was assigned the same frequency as that of rupture of a section of pipe and was included in the frequency of B1. As to bypass by spurious opening of the standby pump isolation check valves, this is also explained in Section 3.1.2. The

Question reference	Section number and name	Topic	ARPANSA Comment, Issue and/or Question and ANSTO's Response
			situation in the PCS is rather different than in the RSPCS (see Figure 3/11 of the PSA). For the PCS, each line with a pump has, besides the check valve, a pair of butterfly block valves. The line that is not in use will be blocked with one or two of these valves, because there is no operation of this branch in any situation. For the next cycle, another pump line will be blocked and so on. This is going to be assured by procedure. Therefore, the possibility of a flow reduction due to bypass implies two serial events, a procedure breaking and a check valve failure. Its contribution to the overall event B2 will be small providing the check valves are tested at least twice each year. At least one of these defences must be functional at start up for power (forced circulation) mode because otherwise the required flow would not be available, and an interlock on low flow or low pressure drop will trip the FSS. If a longer test interval is adopted, the frequency of this event might need to be increased as is suggested. This will be reviewed at the FSAR stage.
PSA.22.	3.1.2 Barriers Failure Mechanism—Uncontrolled reduction of heat removal.	Event B4 is associated with the closure of a primary cooling system isolation valve.	If closed during maintenance, the closure of the valve would be revealed before the reactor was taken to power. It should be established that the valves are not motorised and cannot be remotely operated.

Question reference	Section number and name	Topic	ARPANSA Comment, Issue and/or Question and ANSTO's Response
			Response: The PCS isolation valves are manually operated butterfly valves. Actuation is only by local manual action. Refer to Chapter 6, Section 6.2.5 and Chapter 16, Section 16.9.2.2.1 of the PSAR. The valves cannot be operated remotely.
PSA.23.	3.1.2 Barriers Failure Mechanism—Uncontrolled reduction of heat removal.		The coverage of flow transients is adequate, but it needs to be established that loss of flow transients without operation of the FSS is modelled in the PSAR. An important question is the confidence in the thermal hydraulic and nuclear modelling of the core behaviour (Ch.16 of the PSAR) in the time it takes the SSS to be effective.
			Response: This has been modelled in Chapter 16 of the PSAR. Full credit had been given in the PSA for the SSS, because it is shown in the analysis, that the SRPS/SSS is adequate for all design basis initiators.
PSA.24.	3.1.2 Barriers Failure Mechanism—Loss of Coolant Accidents (LOCA)	LOCAs are a possible source of losing the cooling capabilities of the core. They may also degrade the pool coolant as a barrier to contain the radioactive materials that come from the core. The LOCAs considered are PCS pipework rupture, neutron beam breach, and control rod mechanism breach.	The failure of the neutron beam tubes and control rod drives have been screened out. The number of such penetrations is significant (5 beam tubes, 16 fuel element assemblies, 5 CR assemblies, Reflector Tank Drain line, and instrumentation lines. In view of the numbers involved and the fact that they are not protected by the siphon breaks, the justification for the screening out should be provided. For penetrations into the CRR there is a dependence on the integrity of the CRR.

Question reference	Section number and name	Topic	ARPANSA Comment, Issue and/or Question and ANSTO's Response
			Response: As explained in the PSA (Section 3.1.2 pp 3-10 - 3-11), these events were screened out for the following reasons. Penetrations into the Control Rod Drive Room are by double seals in an assembly around the rod or FA attachment. If these seals were to fail catastrophically, there would still only be a very small flow annulus. The Control Rod Drive Room has a sealed door, which must be shut while the reactor is at power. These features are fully described in the PSAR (Chapter 4, Section 4.5 and Chapter 16, Section 16.11). The neutron beam tubes are high integrity systems with two complete barriers. These are described in the PSAR (Chapter 4, Section 4.5, Chapter 11, Section 11.5.1.4 and Chapter 16, Section 16.15). The design will ensure that catastrophic failure is incredible.
PSA.25.	3.1.2 Barriers Failure Mechanism—Loss of Coolant Accidents (LOCA)	LOCAs are a possible source of losing the cooling capabilities of the core. They may also degrade the pool coolant as a barrier to contain the radioactive materials that come from the core.	Inadvertent drainage of the pool to the drain tank has not been considered. There is a provision for this in order to facilitate inspection of the Reactor Pool. The arrangements for draining should be examined to ensure the pool is not vulnerable to failure of the drainage pipework.
			Response: There is no drain line from the Reactor Pool to the refilling pool so inadvertent drainage is not possible. A submersible pump in the pool is required to drain the pool. This pump discharges to the pool overflow channel from where it drains via the RPHWLS expansion tank to the refilling pool at Level -7. Please refer to Chapter 4, Section 4.5.1.5.2.2 and Chapter 12, Section 12.4.5.3.4 of the PSAR.

Question reference	Section number and name	Topic	ARPANSA Comment, Issue and/or Question and ANSTO's Response
PSA.26.	3.1.2 Barriers Failure Mechanism—Fuel Element Failure or Damage)	There are several potential mechanisms that may cause failure of a single fuel element. Those considered are; mechanical damage, manufacturing failure, and corrosion. All of these are screened out of consideration in the PSA.	Justification for screening out the failed cladding from any of the above mechanisms should be provided, even though the consequences are low and there is no likelihood of significant core damage. A comparison with the HIFAR PSA indicates that more fuel damage mechanisms have been considered.
			Response: Failed cladding in a pool reactor does not result in a dose to the public. The screening out of these events is consistent with the SEA method. The SEA method was systematic and comprehensive. HIFAR is a different type of reactor. Comparison with HIFAR PIEs may not be meaningful. Analysis of many postulated fuel damage mechanisms following the HIFAR PSA showed that there would be no significant consequences. Mechanical fuel damage is analysed in Chapter 16, Section 16.13.
PSA.27.	3.1.2 Barriers Failure Mechanism—Fuel Element Failure or Damage)	The dropping of heavy objects onto the fuel in the core is judged not to be credible in normal operation since a grid protects the core from any falling object.	There is a possibility of dropping objects into the core during shutdown, and possibly during low power operation. The PSA should include coverage of shutdown and low power operation.

Question reference	Section number and name	Topic	ARPANSA Comment, Issue and/or Question and ANSTO's Response
			Response: The chance of dropping objects may be slightly higher during shutdown, but the core is no more vulnerable at this time except during refuelling when the grid will be removed. For major shutdowns, the fuel would be removed from the core. Low power operation mode is carried out with the protective grid in place. Regarding the shutdown state, the geometry of the core and fuel assemblies (control plates guide boxes, handling pin, lateral plates) makes direct damage to the fuel plates highly unlikely. Damage to a plate or several plates would lead to a decrease in cooling arising from the reduction inflow area. No mechanism is envisaged that could cause a generalised damage to the core.
PSA.28.	3.1.2 Barriers Failure Mechanism—Irradiated fuel Assemblies in Services Pool.	Up to 10 years of spent fuel will be stored in the Services Pool. These elements are shielded and cooled by the pool water. The potential mechanisms for fuel damage are: criticality in fuel storage, mechanical damage, corrosion, and failure to remove decay heat. Only mechanical damage (event E1) is treated in the PSA	The exclusion of criticality needs justification, since there is a need to consider the dropping of heavy loads onto the stored fuel, as well as potential spill of elements during spent fuel transfer or from a failure of the racks.

Question reference	Section number and name	Topic	ARPANSA Comment, Issue and/or Question and ANSTO's Response
			Response: The racks will be of solid construction able to withstand dropped assemblies without damage. The moving of heavy loads over the racks will be controlled by administrative procedures. The crane will have an interlock to prevent it from travelling above the reactor pool during manipulation of the spent fuel transport cask (see Chapter 4, Section 4.5.2.1.4 of the PSAR) Radioisotope/silicon operations do not require movement of materials over the spent fuel storage racks. If a rack were crushed, it is unlikely that the cadmium lining which provides engineered protection from inadvertent criticality could be removed. Therefore inadvertent criticality due to such an event is considered incredible.
PSA.29.	3.1.2 Barriers Failure Mechanism—Irradiated fuel Assemblies in Reactor Pool.	After refuelling the fuel assemblies will be stored in storage racks inside the reactor pool for at least 15 days to remove decay heat. The potential mechanisms for damage are: criticality, mechanical damage, corrosion, and failure to remove decay heat. Only mechanical failure (E2) is considered in the PSA.	The exclusion of criticality needs justification, since there is a need to consider the dropping of heavy loads onto the stored fuel, as well as potential spill of elements. More information is also needed on the cooling of the spent fuel if circulation is lost, or the fuel is exposed during a LOCA that drains the pool, but not the core (Credit to Chimney).

Question reference	Section number and name	Topic	ARPANSA Comment, Issue and/or Question and ANSTO's Response
			Response: The racks will be of solid construction able to withstand dropped assemblies without damage. The spent fuel storage racks in both the reactor pool and the service pool incorporate cadmium within the storage racks' structure. This ensures that even in the unlikely event of crushing of the storage racks, criticality will not be achieved. Regarding the cooling of spent fuel, it should be noted that the fuel is "ever-safe" approximately 15 days after being removed from the core. Exposure to the air after this time does not result in over-heating or damage to the fuel. The spent fuel storage racks within the reactor pool are mounted on the base of the pool such that the top of the active part of the FA is at +1004mm. This is 147 mm below the lowest level of the neutron beam tubes and as such, would remain covered even in the event of a LOCA through one of the beam tubes See Chapter 10, Section 10.1, Figure 10.1/6 of the PSAR.
PSA.30.	3.1.2 Barriers Failure Mechanism—Irradiated fuel Assemblies in Reactor Pool.		The PSA should look at potential mechanisms for pulling a hot spent fuel assembly out of the pool, into the transfer hot cell.

Question reference	Section number and name	Topic	ARPANSA Comment, Issue and/or Question and ANSTO's Response
			Response: This was discussed in page 3-13 point (i) of the PSA report. Removal into the hot cell is not possible due to the physical design of the elevator. Such an incident, with consequences to the public, has not occurred in a pool-type reactor,. Also, there is an interlock that inhibits the transport of irradiated material from the pool into the hot cell due to high activity. The provision of such interlock will be included in Chapter 11 in the FSAR. See Chapter 16, Sections 16.15.2.1 and 16.9.4 of the PSAR.
PSA.31.	3.1.2 Barriers Failure Mechanism—Heavy Water	The heavy water in the Reflector Tank may contain significant amounts of radioactive material. It does not contribute to core damage. The damage mechanisms are: Dropped load on Reflector Tank causing a breach, leakage in the pipework system and spurious opening of expansion tank safety valve. Only the leakage considered in the PSA (F).	A check is needed of Ch.16 PSAR to see if the reactivity effects of mixing heavy and light water in the Reflector Tank has been considered. A breach also introduces a mechanism for draining the pool water through the Reflector Tank dump system.

Question reference	Section number and name	Topic	ARPANSA Comment, Issue and/or Question and ANSTO's Response
			Response: A mixture of light and heavy water is less reactive than pure heavy water (see Chapter 5, Section 5.7.5.5.3 of the PSAR on neutronic efficiency of D_2O as a function of its purity). The reflector tank dump system is sealed except for the header tank. Hence, a breach in the reflector tank would not be a means of draining the pool.
PSA.32.	3.1.2 Barriers Failure Mechanism—Irradiated Materials in the Irradiation Facilities	Some radioactive materials in the irradiation rigs have the potential to release radioactivity. The mechanisms are; uncontrolled power increase, loss of flow blockage of a rig channel, total loss of flow, and loss of cooling in transit to the Hot Cells. Three events are considered G1, G2 and G3, but the uncontrolled power increase is not considered.	The consequences of an uncontrolled power increase on the irradiation targets should be considered in the PSAR. The consequences may not be bounded by A1 and A2.
			Response: A1 and A2 are uncontrolled power increases that are considered to be the most severe. Chapter 16, Section 16.8 of the PSAR includes rig/targets cooling effects. See Figure 16.8/5b.

Question reference	Section number and name	Topic	ARPANSA Comment, Issue and/or Question and ANSTO's Response
PSA.33.	3.2 External Initiating Events	Each external hazard was identified and screening criteria were used as follows: Event of lesser or equal damage potential to events for which plant designed. The event has a significantly lower frequency of occurrence than other events with similar consequences. The event cannot occur close enough to the plant to affect it. The event is included in the definition of another event	The screening criteria used for not considering some external events should be justified. This becomes more important if the bottom line CDF is in the range 10^{-7} to 10^{-8} per year, since rare external events become more important at this frequency range.
			Response: The screening criteria used are based on IAEA guidance set out in their Safety Series. International practice is to utilise a frequency cut-off for external events of 10^{-6} to 10^{-7} per year with seismic events not being considered below 10^{-4} per year. Please see CSNI Report No. 177, '*Consideration of Quantitative Safety Guidelines in Member Countries*', OECD/NEA October 1990. Such events satisfy the ARPANSA dose-frequency criteria without the need to consider consequences.
PSA.34.	3.2.1 Aircraft Crashes	The probability of an aircraft crashing is give in the HIFAR PSA (section 6.3). It is estimated to be $1.8*10^{-7}$ per year. It is a design requirement that the reactor facility buildings and structures be capable of withstanding the crash of a light aircraft without damaging the reactor.	There is a need to consider the aircraft crash contribute if the bottom line CDF is in the range 10^{-7} to 10^{-8} pear year. Rare external events, such as aircraft crash, become more important at this frequency range.

Question reference	Section number and name	Topic	ARPANSA Comment, Issue and/or Question and ANSTO's Response
			Response: Please see response to Question PSA.33.
PSA.35.	3.2.2 Bushfire	ANSTO emergency preparedness arrangements and calculations (Beattie) have been used to argue that a bushfire cannot damage the reactor. Bushfires are not considered in the PSA.	A bush fire is a frequent external event at the LHSTC, with a frequency of 10^{-1} in the area. While a bush fire may not threaten the reactor building, it could effect essential services such as water and electricity, and require the sealing of the containment to prevent sucking in smoke and fire embers.
			Response: The appropriate response to bush fires will be determined in the detail engineering phase. It is expected that the same approach will be adopted as for HIFAR. That is, a precautionary shutdown of the reactor which can then be safely maintained in a cooled condition without power, air or water supplies (See Chapter 16, Section 16.17 of the PSAR).
PSA.36.	3.2.3 Industrial Activities	The review in the HIFAR PSA indicated that there are no industrial activities that posed a hazard to the reactor.	If the bottom line CDF is in the range 10^{-7} to 10^{-8} per year justification for exclusion of consideration of such rare external events is required.
			Response: please see response to Question PSA.33.
PSA.37.	3.2.4 Military Activities	The Holsworthy Military Training Area is close to the LHSTC. The analysis in the HIFAR PSA show that the frequency of a shell hitting the RCB is estimated to be less than 10^{-7} per year. Due the low frequency the military activity was screened out.	If the bottom line CDF is in the range 10^{-7} to 10^{-8} per year, justification for exclusion of consideration of such rare external events is required.
			Response: please see response to Question PSA.33

Question reference	Section number and name	Topic	ARPANSA Comment, Issue and/or Question and ANSTO's Response
PSA.38.	3.2.6 On-site Activities	The results of the HIFAR PSA indicated that there are no potential threats to HIFAR habitability from activities at the LHSTC in general. It is stated that the HIFAR Safety Document (HSD) and HIFAR PSA has not identified an sequences that could impact on the safety of the HIFAR core.	There are activities associated with radioactive materials in buildings 23 and 54, that could threaten the HIFAR and RRR habitability and require evacuation to the Emergency Control Room. The reactor would need to be shutdown. It is not correct to say the HIFAR PSA or HSD has not identified core damage sequences. The HIFAR PSA has estimated the HIFAR CDF as about $2.6*10^{-4}$ per year, which is significantly greater than the RRR CDF estimate.
			Response: The potential for accidents in Buildings 23 and 54 that could threaten the habitability of the Main Control Room of the Replacement Reactor is considered very small. The MCR is well shielded. In the highly unlikely event that the MCR were to require evacuation, sufficient warning would be available to ensure the timely shutdown of the reactor and its continued cooling. Accidents in other buildings on the Lucas Heights site are not considered to pose a risk to the safety of the reactor.
PSA.39.	3.2.7 Extreme Winds	The RRR will be provided with a massive containment structure, and all the critical components will be located within the containment. Extreme winds not included in the PSA.	If the bottom line CDF is in the range 10^{-7} to 10^{-8} per year justification for exclusion of consideration of such rare external events is required.
			Response: Please see response to Question PSA.33.

Question reference	Section number and name	Topic	ARPANSA Comment, Issue and/or Question and ANSTO's Response
PSA.40.	3.2.8 Seismic Activity	The seismic hazard at LHSTC was re-assessed as a follow up to the HIFAR PSA by IGNS. The IGNS report and the peer reviews of it resulted in a peak ground acceleration of 0.3 g for SL-1 2 and a 0.09g for SL-1 (see fig 3/21).	It is noteworthy that the IGNS response seismic hazard curve has been used in the PSA , but normalised to 0.3g PGA. The design (Ch.4 of the PSAR) uses the US NRC RG1-60, normalised to 0.3 PGA).
			Response: It is standard practice in PSA to use the PHGA as the parameter of fragility. This is because the design takes account of the spectrum at each return period.
PSA.41.	3.2.8.3 Seismic Analysis	The seismic hazard is considered as the initiator of several possible accident sequences , such as LOCAs and loss of flow accidents (LOFA). Structures systems and components (SSC) important to safety have been designed at Seismic Category 1 and their seismic fragilities estimated.	The treatment of seismicity in the PSA is important since it could be a mechanism for common cause failure of shutdown systems (FSS and SSS), coinciding with a LOFA and a LOCA. Consideration will need to be given to seismic qualification of key components involved in shutting down the reactor and removing decay heat.
			Response: All Seismic Class 1 items (listed in Chapter 2, Table 2.5/2 of the PSAR) will be seismically qualified to the SL-2.

Question reference	Section number and name	Topic	ARPANSA Comment, Issue and/or Question and ANSTO's Response
PSA.42.	3.2.8.4 Fragility and Component Failure Probability	The seismic fragility of a component is expressed as the conditional probability of a failure for a given peak ground acceleration. A log normal distribution is used. A quantity of some interest is denoted the HCLPF (high confidence of low probability of failure). It is the value for which there is a 95% confidence that there is no greater than a 5% chance of failure. The HCLPF values used were generally taken from the HIFAR PSA	While it is a useful source of information on HCPLF and the associated Beta factors the HIFAR PSA is specific to HIFAR SSC. RRR specific Beta factors should be determined since they are both component and site specific.
			Response: The selected values of β_R and β_U are reasonable for this analysis at the end of the preliminary engineering stage. These parameters will be reviewed in the FSAR stage.
PSA.43.	3.2.9 Conclusions on external initiators	No significant credible external initiators gave been screened out. After examination only seismic events included.	The treatment of external events and their screening out has been discussed above. A whole range of external events has been screened out, and thus will have no contribution to the low CDF estimated (10^{-7} to 10^{-8} per year). The following have been excluded from consideration in the PSA: bushfire, internal fire, internal flooding, on and off-site industrial activities, transportation, and extreme winds. Only seismicity is considered. The HIFAR PSA had considered all of these.

Question reference	Section number and name	Topic	ARPANSA Comment, Issue and/or Question and ANSTO's Response
			Response: HIFAR is reliant on external services to ensure continued cooling of the core following shutdown. The HIFAR PSA investigated the potential for these to fail. In the case of the RRR, no external services are necessary to ensure the safe shutdown of the reactor and continued cooling of the core and rigs. Moreover, internal fire and internal flooding are not external initiators.
PSA.44.	3.3 Selection and Grouping of Initiating Events	Table 3./1 lists the initiating events considered . The sequences contributing to CDF are two reactivity transients, five loss of flow accidents, three loss of coolant accidents, and a loss of heat sink. Seismic events are also considered as a CDF contributor.	The list in Table 3.1 is a result of a screening process described above. The justification for excluding events, which were contributors to the HIFAR PSA, should be provided.
			Response: The determination of initiating events was based upon IAEA guidance together with consideration of the design of the RRR. HIFAR is different from the RRR and not all HIFAR initiators are relevant to the RRR. See responses to Questions PSA.33 and PSA.43.

Question reference	Section number and name	Topic	ARPANSA Comment, Issue and/or Question and ANSTO's Response
PSA.45.	3.3 Selection and Grouping of Initiating Events		A number of important operating modes and leak sequences have not been covered. These include: • Accidents at shutdown and low power when the levels of protection may be degraded. • Direct leakage pathways from the primary circuit by means of heat exchanger leaks. • Loss of electrical services to release mitigation systems, such as containment energy removal and post accident monitoring systems.
			Response: As is standard practice, preliminary PSA covers only start up and power operation modes. However, analysis of low power events will be provided. Direct leakage pathways from the primary circuit by means of heat exchanger leaks are considered in Chapter 16, Section 16.11 of the PSAR. Release mitigation systems such as containment energy removal and post accident monitoring are supplied by standby Diesel generators, with very low failure frequency.
PSA.46.	3.3.1 and 3.3.2 Reactivity Transients A1 and A2	Both transients include the uncontrolled extraction of a single control rod, either during reactor Start-up or in normal operation. The transient is a ramp and not a step, since rod assumed driven out at maximum velocity.	There is no consideration of a sudden ejection of a control rod (step change) or the removal of the whole bank of rods simultaneously. The design is claimed to make these sequences incredible, but this needs detail justification for all operating modes of the reactor.

Question reference	Section number and name	Topic	ARPANSA Comment, Issue and/or Question and ANSTO's Response
			Response: The design of the Control Rods and their Guide Boxes ensures that the flow of coolant over them cannot lead to the ejection of a Control Rod even in the event of a shaft failure. See Section 5.4. Bank withdrawal of Control Rods is prevented by independent hardwired devices. The probability of their failure is less than 10^{-6} per year, rendering the likelihood of the sequence beyond the design basis. The interlock and hardwired devices are operative at low power and full power operation modes.
PSA.47.	3.3.3 to 3.3.7. Loss of Flow Events (LOFA)	Five events are described covering: core bypass, loss of power supply, primary pump failure, primary isolation valve closure, and fuel channel local blockage.	The treatment of LOFAs is satisfactory. An important issue is the confidence that can be placed in the thermal hydraulic regime in the core should the FSS fail , and reliance is placed on the SSS to shutdown the reactor (refer to Ch.16 of the PSAR and its supporting documents).
			Response: In Chapter 16 of the PSAR, loss of flow events are analysed with failure of the FSS. The resulting temperatures are below saturation so the thermal-hydraulic regime is the same as during power operation. Not withstanding this the correlations and models used for conditions above saturation are considered to be appropriate. ANSTO will perform an independent review of these analyses.
PSA.48.	3.3.8 to 3.3.10 Loss of Coolant Accidents (LOCA)	Three events describe LOCAs in the; primary circuit upstream of the primary pump, primary circuit downstream of primary pump, and pipe rupture in the pool cooling system.	Major failures of the penetration system leading to LOCAs have been screened out. These are generally below the core, and depend on other design features such as the Control Rod Room integrity to prevent draining the core. Justification for this is required.

Question reference	Section number and name	Topic	ARPANSA Comment, Issue and/or Question and ANSTO's Response
			Response: See response to Question PSA.24.
PSA.49.	3.3.11. Loss of Heat Sink	This represents a total loss of heat extraction by the secondary cooling water (SCW).	The SCW is not an ESF and is designed as a Safety Category 2 system. Its failure should be anticipated beyond SL-1 seismic events.
			Response: Yes, the SCW is not an ESF. However, the Secondary Cooling System equipment and piping for long term pool cooling is Seismic Class 1 (Ref Chapter 2, Table 2.5/2 of the PSAR). Failure at the SSE would have a very low probability. Failure probability even up to extreme events at 0.8 g would be about 50%.
PSA.50.	3.3.12 to 3.3.14 Fuel Assembly Mechanical Damage	Three sequences are described involving damage in the service pool, reactor pool and while in transit .	Only mechanical damage considered from dropped loads etc. There is no consideration of uncontrolled criticality from dropped loads or from spillage from storage racks.
			Response: Please see responses to Questions PSA.28 and PSA.29.
PSA.51.	3.3.19 Seismic Event	A seismic event is assumed to result in loss of mains power, mains water, the LHSTC water tower. The RRR does not depend on these services to remove decay heat	The seismic contribution to LOCA and LOFA could be important for events beyond the SL-2 for which Safety Category 1 systems are designed. There are also some common cause failure considerations with respect to the FSS and SSS in very large seismic events.
			Response: Please see response to Question PSA.33

Question reference	Section number and name	Topic	ARPANSA Comment, Issue and/or Question and ANSTO's Response
PSA.52.	3.4 Evaluation of Initiating Event Frequencies	For estimating the initiating event frequencies it is assumed the reactor operates for 33 days, with 2 days shutdown.	The operating cycle means there is very little time for maintenance (22 days per year) and fuel change operations. The 33 days operation could have some implications on the fuel loading (eg need for burnable poisons). This suggests that consideration of transients should be at the beginning of the cycle (BOC), with FSS minimum absorption capability (assuming maximum control rod burn-up).
			Response; The failure at start up means no xenon poisoning and hence, the minimum reactivity inventory in the control plates in that position. The fuel incorporates burnable poison
PSA.53.	3.4.2 Failure Models and Identifiers	Failures are consider to occur in a "failure on demand mode" and failures " in a non demand mode". (see Table 3/3)	The failures in the non-demand mode presumably mean that they are not revealed until a test or real demand. The test interval could thus be an important factor in establishing SSC reliability and performance.
			Response: The non-demand failure mode is applied to events where the failure probability over a mission time needs to be estimated. That is the case, for example, to estimate many of the IE frequencies. The mission times used were the annual operating times of the pumps and fans as given in Table 3/2 of the PSA. These items are operating items not stand-by items which were modelled either by • "on-demand" failure probability, or • "unrevealed" failures with appropriate test intervals (tau). Nevertheless, it is recognised that test intervals will be an important factor in establishing safety system reliability and performance.

Question reference	Section number and name	Topic	ARPANSA Comment, Issue and/or Question and ANSTO's Response
PSA.54.	3.4.3 Erroneous Withdrawal of a Control Rod during Start-up—A1	The start up period lasts 10 hours and planned start-ups occur 11 times a year. The reactor is on natural circulation at the beginning of start-up. The assumption is that the heaviest rod (4000pcm) is withdrawn at the maximum speed (20 pcm/sec). Both the FSS (FRPS) an SSS (SRPS) detect the high neutron flux. The mean annual failure probability is estimated as $5.3*10^{-5}$ per year.	The failure rate is based on planned start-ups only and does not seem to include trip recovery situations. It is also based on generic information(IAEA TECdoc-478-p118) and a quoted failure rate of $9.7*10^{-8}$ per hour. The validity of these assumptions needs independent checking and comparison with similar reactors.
			Response: This will be reviewed in the FSAR stage. It is not expected to make a significant difference to the overall CDF. Availability design target and contract specifications require very low frequency of spurious trips (Design target is less than 1 per year during normal operation). For example many nuclear power plants around the world have less than 1 unplanned reactor trip per/year.
PSA.55.	3.4.3 Erroneous Withdrawal of a Control Rod during Normal Operation—A2	The period lasts 8159 hours and planned start-ups occur 11 times a year. The assumption is that the heaviest rod (4000pcm) is withdrawn at the maximum speed (20 pcm/sec). Both the FSS (FRPS) an SSS (SRPS) detect the high neutron flux. The mean annual failure probability is estimated as $8*10^{-4}$ per year.	The only difference between A2 and A1 is the number of hours in these modes (8259 hrs and 110 hrs). It is not clear why there is a factor of 15 difference between the failure probability when the time ratio is a factor of 75.

Question reference	Section number and name	Topic	ARPANSA Comment, Issue and/or Question and ANSTO's Response
			Response: A further factor of 5 arises because in the "At power" situation (A2), four of the five rods would be effectively fully withdrawn. The case is treated conservatively in that the 5^{th} rod which is postulated to be erroneously withdrawn was deemed to have the same worth as the heaviest absorber, but in reality, it would be the centre absorber which has a lesser worth.
PSA.56.	3.4.5 Loss of Flow—Core Bypass—B1	This event consists of a core bypass in the part of the PCS which is located inside the reactor pool, and reduces flow through the core at full power.. the spurious opening of a flap valve, or PCS pipe failure are suggested as reasons. Both the FRPS and SRPS detect "low core pressure difference" signal to trip the reactor. The total annual failure probability is estimated as $7.4*10^{-5}$.	The failure rate is based on 1 $*10^{-10}$ per hour (8.76 $*10^{-7}$ per year—IAEA TECDOC-478—P158). It appears a value of 9 times this was actually used The usual value used for pipe work is closer to 10^{-4} to 10^{-5} per year—see HIFAR PSA Table 5.4.1. The failure rate assumptions need to be justified.
			Response: The HIFAR values were based on the Thomas model and represent a summation over all the pipework. The data used for the RRR PSA came from accepted IAEA reports and are based upon lengths of pipe. The total frequencies of pipe failure for the RRR vary from 0.6 to 1.3 x 10^{-4} per year. There are no inconsistencies between the two sets of data

Question reference	Section number and name	Topic	ARPANSA Comment, Issue and/or Question and ANSTO's Response
PSA.57.	3.4.6 Loss of Main Power Supply—B2	The loss of mains supply is not unexpected. The annual frequency is taken from the HIFAR PSA Table8.8 and quoted as $2.83*10^{-1}$ per year	The value for loss of offsite power quoted from HIFAR PSA is based on a sustained loss of off-site power (order of hours) The value that should be used is for power interruptions which cause the pumps to trip. The frequency is 1.89 events per year, or about a factor of 10 higher. This is in line with HIFAR experience over the past 40 years. The failure rate for B2 should be justified.
			Response: From an initial review of the data analysis in the HIFAR PSA, it would appear that some fraction of the 1.89 events per year might arise from old distribution equipment (since different values are quoted at different MCCs). This would not be applicable to the RRR. Nevertheless, the assigned frequency for the event B2 will be revisited with a view to its modification. As an exercise, the effect on CDF of a frequency for B2 of 1.89 pa was assessed. It was determined that it would increase the overall CDF by about 7.5%. The initiating event frequencies will be reviewed in the FSAR stage.
PSA.58.	3.4.7 Primary Pump Failure—B3	This event represents the malfunction of one pump when the reactor is operating at full power. The IAEA generic failure rate (IAEA TECDOC-478—p161) is $6.2\ 10^{-6}$ per hour or $6.7*10^{-2}$ per year.	The value is lower than HIFAR experience (Table 8.8 of HIFAR PSA gives $1.2*10^{-1}$), which is probably more representative of ANSTO operations. The failure rate for B3 should be justified.
			Response: The HIFAR value is based on a Bayesian update of generic data while the value used for the PSA is based solely on generic data. The two values are within a factor of 2, which is considered acceptable at this time

Question reference	Section number and name	Topic	ARPANSA Comment, Issue and/or Question and ANSTO's Response
PSA.59.	3.4.8 Primary Isolation Valve Closure-B4	This event represents closure of one of the PCS isolation valves when the reactor is operating at full power. Following maintenance a human error is the most likely cause. The estimate is $2.8*10^{-4}$ per year.	The failure rate is probably ok since the closure can only occur during maintenance, and would be revealed during reactor start-up by the low flow in the PCS. The only concern would a remote operation (motorised valve) which would permit easy closure during operation.
			Response: See response to Question PSA.22.
PSA.60.	3.4.9 Fuel Channel Blockage-B5	This event does not lead to core damage so not considered in the PSA.	What is the potential for some fuel plate damage, depending on the blockage and subsequent behaviour of the fuel. Have other mechanisms for partial fuel damage also been considered, such as flow induced vibration and mechanical damage during fuel loading.
			Response: The analysis of channel blockage has been done for two different cases with the following assumptions: 1) The whole length of a fuel channel is blocked, with a piece that enters 2.5 cm into the channel. This case is worse than the tangential blockage of the channels, with no intrusion of the blocking object into the channel, because it leads to lower coolant velocities in the blocked channel (See Figure in Appendix PSA.1. 2) A single channel is completely blocked. The heat removed by counter current flooding mechanism is conservatively neglected, then the two adjacent channels receive a heat flux which is 50 % larger than the normal one. The local heat flux at the plate in contact with the blocked channel doubles with respect to the normal heat flux The results for case 1 (See Appendix PSA.1) show that for blockages of as much as half the flow area of the channels,

Question reference	Section number and name	Topic	ARPANSA Comment, Issue and/or Question and ANSTO's Response
			the margins to critical phenomena are above the safety limit. ONB is attained for blockages greater than 30 % of flow area. The fuel plate wall temperature is well below design limits (blistering temperature is 450°C) for all cases. The results for Case 2 (Appendix PSA.1) show that the maximum plate wall temperature in contact with the blocked channel reaches a value of 252°C, which is also well below design limits. The channels adjacent to the blocked one attain ONB conditions. The core is designed to have a velocity below the safety limit of 2/3 of the critical velocity (see Chapter 5, Table 5.8/4 of the PSAR). The design of the fuel assembly is being hydraulically tested in the detail engineering phase. Therefore, there is no physical mechanism that can provide a flow large enough to trigger flow induced vibration damage. Mechanical damage during fuel loading is discussed in Chapter 16, Section 16.13 of the PSAR.
PSA.61.	3.4.10 Primary LOCA Caused by a Rupture Upstream of a Primary Pump.—C1	This LOCA causes the PCS pumps to cavitate as well as lowering the level of pool water until the siphon breakers take effect. The value used is $5.9*10^{-5}$ per year, which includes all the relevant pipe work on Fig 3/11.	A common value used for pipe work is close to 10^{-4} to 10^{-5} per year - see HIFAR PSA -Table 5.4.1 . The failure rate assumptions are similar to HIFAR.
			Response: Comment noted.

Question reference	Section number and name	Topic	ARPANSA Comment, Issue and/or Question and ANSTO's Response
PSA.62.	3.4.11 Primary LOCA Caused by a Rupture Downstream of a Primary Pump.—C2	This LOCA does not cause the PCS pumps to cavitate, but lowers the level of pool water until the siphon breakers take effect. The value used is $1.2*10^{-4}$per year, which includes all the relevant pipe work on Fig 3/11.	A common value used for pipe work is close to 10^{-4} to 10^{-5} per year - see HIFAR PSA -Table 5.4.1. The failure rate assumptions are similar to HIFAR.
			Response: Comment noted.
PSA.63.	3.4.12 Reactor and Service Pools Cooling System LOCA—C3	A LOCA would dump pool water until the siphon effect breakers actuate. The value used is $1.3*10^{-4}$ per year, which includes all the relevant pipe work on Fig 3/16.	A common value used for pipe work is close to 10^{-4} to 10^{-5} per year - see HIFAR PSA -Table 5.4.1. The failure rate assumptions are similar to HIFAR. Note no consideration given to beam tube and other penetration failures that could drain the pool.
			Response: The design provisions, multiple barriers, material quality, and QA manufacturing and installation procedures in place for the beam tubes are such that the likelihood of failure of the beam tubes is so low as to render it beyond the design basis. The only other penetrations to the pool are those associated with the fuel and CRs through the bottom of the pool. The seals employed and the design of the watertight door to the Control Rod Drive Room are such as to preclude the likelihood for the draining of the pool by this route (see response to Question PSA.24).

Question reference	Section number and name	Topic	ARPANSA Comment, Issue and/or Question and ANSTO's Response
PSA.64.	3.4.13 Loss of Heat Sink--D	This event leads to a total loss of heat extraction via the Cooling Towers. Loss of electric power not considered since covered in B2. The total annual failure is estimated as 4 $*10^{-2}$ per year.	It is not clear that B2 bounds this event since clearly a loss of offsite power involves a loss of secondary cooling and should be included. More justification is required. This is also related to the discussion about the value used for the B2 loss of power probability. The HIFAR PSA value for sustained loss of power has some relevance to sequence D , ie. $2.83*10^{-1}$ per year and should be included in the estimate.
			Response: It is not claimed that B2 bounds this event. Event B2 includes loss of mains power to all systems. Event D covers all cases where there is loss of secondary cooling but not (necessarily) a loss of PCS flow. In event D, the RPS1 would be required to call on the FSS to shutdown the reactor, whereas in B2, the FSS would actuate by loss of power to the CRD magnets. Event D does not include loss of Mains power supply because that would double count the IE. .
PSA.65.	3.4.14 to 3.4.16 Fuel Assembly Mechanical Damage—E1 to E3	These events not included in the PSA since they do not contribute to the core Damage Frequency (CDF)	The events E1to E3 and F, G1,G2,and G3) do not contribute to CDF, but need to be included for any PSA Level 3 Considerations.
			Response: The offsite consequences of events E3, G1, G2, and G3 were considered in the PSA. The associated likelihoods and consequences are reported in Chapter 7. The consequences of the remaining events were not determined as they are considered minor; having no offsite impact.

Question reference	Section number and name	Topic	ARPANSA Comment, Issue and/or Question and ANSTO's Response
PSA.66.	3.4.21 Seismic Event	The IGNS estimate of seismic hazard is used (Table 3 /4 and Fig 3/21), but scaled to 0.3 g PGA. The mean seismic hazard curve was used	The PSA uses the IGNS PGA return period recurrence curve. This may not be consistent with the methods adopted for the seismic design in Ch.4 PSAR since US NRC guidance used.
			Response: These are two different points. One is the PGA return period recurrence that has been taken from IGNS to reflect the "probability distribution of earthquakes in the area", and the other is the design spectrum taken from USNRC as an appropriate bounding shape that is used worldwide to analyse seismic events at nuclear power plants. The USNRC spectrum is anchored at 0.3g to reflect the specific potential of the LHSTC area.
PSA.67.	4 Event Tree Headings	The event tree headings are described and cover all the safety systems that either shutdown the reactor or remove decay heat. They include the FRPS, SRPS, SSS, FSS, Flap valves and Siphon Effect Breaks, and Standby Power System. Success criteria are specified for each event tree and the modelling is generally based on Failure modes and Effect Analysis.	The event trees only consider systems or components that either shutdown the reactor or remove decay heat. There is no consideration of the containment or post accident monitoring, and the Standby Power Supply is only required in as far as it is required for operation of the Second Shutdown System (SSS).
			Response: The PSA concentrated upon the determination of the likelihood of release of radioactive material. The determination of consequences for the selected fault sequences was carried out in a very conservative manner. The results show that the risks associated with the operation of the RRR are very low. Consideration of failure of the containment would not change those conclusions.

Question reference	Section number and name	Topic	ARPANSA Comment, Issue and/or Question and ANSTO's Response
PSA.68.	4.1.1 First Reactor Protection System (FRPS)	The FRPS is a software based system and is responsible for the detection of safety variables and the generation of the actuation signals for the FSS. The success criteria is the detection of the postulated failure and the sending of the actuation signal to the FSS. The design or (hidden) failure of the software is assumed to dominate, and a conservative unavailability of 10^{-3} is assumed. The detection part of the FRPS is triplicated, and uses a two-out of three logic for the generation of safety signals.	The FRPS unavailability assumed is at the lower end of the range expected for a first level protection system It is however a reasonable value in view of the reliance on software. There is no discussion of low power operation and what parameters are excluded in this mode. Also, it would appear that there is no trip associated with the loss of heat sink, other than core temperature increase.

Question reference	Section number and name	Topic	ARPANSA Comment, Issue and/or Question and ANSTO's Response
			Response: The Safety Integrity level (SIL) for software based safety systems is generally assigned a 10^{-3} to 10^{-4} unavailability rating. It should be noted that triple modular redundant TMR designs such as the Tricon are generally thought to provide enough redundancy to warrant a higher rating (per section 7.4.5 of ISA Safety Shutdown Systems by Paul Gruhn and Harry Cheddie). The FRPS has been assigned the more conservative value. Additionally the Triconex has over 100,000,000 hours of error free operation. At this time the parameters that are blocked when in the low power operational mode are the core delta P and the low flow trip. These can be seen in Chapter 8, Figure 8.2/13 of the PSAR. It is expected that the full power trip parameters for the nucleonics will be switched to a second set of low power trip parameters. This mode of operation will be developed during the detail engineering phase. There are three separate trips associated with core temperature increase. Two for the FRPS and one for the SRPS.

Question reference	Section number and name	Topic	ARPANSA Comment, Issue and/or Question and ANSTO's Response
PSA.69.	4.1.2 Second Reactor Protection System (SRPS).	The SRPS is a hard-ware based system. It is independent from the FRPS, both in sensors and logic. The number of trip parameters is less than for the FRPS, but covers neutron flux, low core pressure difference, low pool water level, high seismic level, high reflector vessel water temperature and failure of the FSS. The success criteria are the detection of the postulated event and the generation of an SSS actuation signal. The detection part is triplicated using a two-out of three logic through dedicated hardware. The unavailability value specified for the SRPS is 10^{-4}.	It is stated that FSS failure is a trip parameter, but it appears FRPS success is required to generate this signal. This could be a problem since the FRPS is less reliable than the SRPS, and the interconnection between them is a degradation of separation and independence. If the number of parameters on the SRPS was increased there may be no need to have this interconnection. It is also questionable to have the more reliable SRPS associated with the slower SSS, and the less reliable FRPS associated with the faster FSS. It is also not clear whether the FRPS and SRPS use different sensors for the parameters they share.

Question reference	Section number and name	Topic	ARPANSA Comment, Issue and/or Question and ANSTO's Response
			Response: The FRPS will be a very reliable system. The quantified reliability used for the PSA is considered very conservative. The connection between the FRPS and the SRPS is optically isolated and does not represent a degradation of separation and independence between the two systems. Where the FRPS and SRPS utilise the same process parameters to initiate a reactor trip, those parameters are obtained from different sensors. It is true that the SRPS trip on failure of the FSS requires the FRPS trip signal to be generated. This trip is to backup a failure of the FSS not a failure of the FRPS trip. A failure of the FRPS to initiate a trip is accounted for by the SRPS and the SSS and its diverse and independent instrumentation. The failure of the FRPS is addressed in the previous question. There is no degradation, or problems with independence or separation, in having the signal from the FRPS feed the SRPS, to arm the FSS fail circuit. The signals are isolated to IEEE 384 requirements as are all the FRPS, SRPS and PAM signals that feed the RCMS. For the SRPS to trip on a failure of the FSS, requires a signal from the FRPS to show that it has demanded a FSS trip. There are no other parameters, which can duplicate this signal. This is not a failure of the FRPS feature but a failure of the FSS to drop the rods properly.

Question reference	Section number and name	Topic	ARPANSA Comment, Issue and/or Question and ANSTO's Response
PSA.70.	4.1.2 Second Reactor Protection System (SRPS).		The number of trip parameters that are in the FRPS, but not in the SRPS needs justification. How important to their selection is the wish to avoid "poison out" or slow trip recovery due to the time it takes to refill the reflector tank.
			Response: Only those actions that protect from damage to the core have been diversified.
PSA.71.	4..2 First Shutdown System (FSS)	THE FSS consists of gravity driven insertion of five control rods, with compressed air assistance to fulfil the injection in less than 1 second. The success criteria is the full insertion of any four of the five rods within one second.	More information is needed on the importance of the air assistance to FSS success. The FSS should be shown to be successful, both in drop time and absorption capacity, for all transients in Ch.16 of the PSAR, without the air assistance if it is to be claimed "fail safe".
			Response: The FSS is fail safe in the sense that loss of power, either total power to the plant or local power to the pneumatic valves, releases the compressed air to provide assistance to FSS operation. However, it is noted out that failure of the air assistance is considered, in the safety analysis of Chapter 16 of the PSAR, as a total failure of the FSS. In this case the actuation of the SSS is taken into consideration. The SSS is able, by itself, to shutdown the reactor in all postulated transients. Also note the Design Bases for the FSS (Section 5.5.3.2, item (a) of the PSAR), calls for the insertion of 2000 pcm in 0.5 sec, a value that will be fulfilled. A preliminary assessment of the FSS design is included in Chapter 5, Section 5.7.5.4.1.1 and Table 5.7/18 of the PSAR.

Question reference	Section number and name	Topic	ARPANSA Comment, Issue and/or Question and ANSTO's Response
PSA.72.	4..2 First Shutdown System (FSS)	Figures 4/2 to 4/9 show the development of the FSS Fault Trees. The mean failure on demand of the FSS is claimed to be $4.1*10^{-5,}$ which is made up of a rod insertion failure of $3.9*10^{-5}$, and a compressed air supply failure of $1.7*10^{-5}$. The individual rod insertion failure is estimated to be $8.2*10^{-5}$.	The rod insertion failure values require justification. Where available, information should be obtained from experience in similar designs in other reactors rather than relying on FMEA evaluation (See Ch.2 PSAR and Proven Design"). The value for the failure of the air system also requires justification, in view of its complexity and exposure to maintenance error. In Fig 4/8 it would appear that combined maintenance and test (Type M and T) errors are multiplied together to give a value of around 10^{-6}, which as discussed earlier should be justified.
			Response: The rod insertion failure values derive from IAEA TECDOC 478 (which derives from PWR control rod and drive mechanisms). This value is reasonable. The value did not derive from FMEA, rather, the FMEA was used to assure the designers that there was no unusual failure modes. The air system is relatively simple and has been modelled with particular conservatism. It is provided with a set of alarms that indicate its availability to the operator. The control rod drives are located in an exclusive room, they are accessible for maintenance and tests and they are not underwater. The rods are fully guided from the CRD to the reactor core. In Figure 4/8, the maintenance and test (type M and T) errors feed into an OR gate and the net effect is to add their failure probability to give a probability of failure of around 2.2×10^{-3}. There is no occurrence of type M and type T errors feeding into an AND gate in the FSS or elsewhere in the PSA.

Question reference	Section number and name	Topic	ARPANSA Comment, Issue and/or Question and ANSTO's Response
PSA.73.	4.2.6 FSS Seismic Considerations	The FSS has been designed to withstand the SL-2 seismic event. The active components of the FSS are assumed to be vulnerable to seismic failure, and includes valves in the compressed air system and the control rods. For the seismic event it is claimed that 1 second drop is not important, so loss of air is not important.	It is not clear how the seismic failure has been modelled, and whether gross failure is considered, eg by distortion of the chimney or anchorage failure in the CRR which prevents any of the plates dropping in. Seismic testing of the CRs is important to establish a specific seismic fragility for the FSS.
			Response: Seismic failure of control rods to insert was taken into account. The HCLPF value is at ground motion of 0.3 g, as with other Seismic Class 1 items (Refer to Chapter 2, Table 2.5/2 of PSAR). Gross failures of the chimney, or CRDM anchorages were not considered because of the extremely robust design. All Seismic Class 1 items are to be seismically qualified.
PSA.74.	4.3 Second Shutdown System (SSS)	The SSS consists of a gravity–driven dump of the reflector vessel to the drain tank in 15 seconds. The negative reactivity insertion is 3000 PCM in 15 seconds. The action of the dump is by means of six valves, five of which need to open for success. The Fault Trees are shown in Fig.4/11 to 4/17 and the mean failure probability was estimated as $3.2*10^{-4}$.	It would appear that five out of six of the drain valves would need to open for success. There should be tests done to establish the drain time with all the combinations of valves opened and closed
			Response: The success criteria for the SSS is for 5 out of 6 drain valves to open as stated in Chapter 5, Section 5.5.4.5 of the PSAR. Tests have been performed with varying valve combinations and will be reported in the FSAR.

Question reference	Section number and name	Topic	ARPANSA Comment, Issue and/or Question and ANSTO's Response
PSA.75.	4.3 Second Shutdown System (SSS)	The solenoid valves that vent the air will open on a lack of power. To prevent spurious actuation of the SSS; the solenoid valves are energised by UPS category 1.	The SSS is not fail-safe on a loss of power to the same extent as the FSS. The system is kept closed by the UPS, and is only fail safe on loss of UPS. This adds complexity to the operation of the SSS. Is the wish to avoid "poison out" or slow trip recovery, due to the time it takes to refill the reflector tank, the reason for not dumping on loss of power.
			Response: The SSS is fail-safe on loss of power but is not tripped on loss of off site power. There is no added operational complexity in this design. There is a loss of power signal that feeds the FRPS, which in turn sends an isolated trip signal to the SRPS. The FSS magnets will be de-energised as a direct result of loss of offsite power as power to the FSS is not from the Standby Supply. If 2 or more rods do not reach bottom then the SRPS will trigger the SSS. Yes, the design intent is to limit the number of unnecessary SSS trips thereby limiting the poison outs. See the response to Question 5.91.
PSA.76.	4.3 Second Shutdown System (SSS)	Closure of valve 0310-VF-010 during maintenance or testing could leave the SSS disabled.	There is a single isolation valve (0310-VF-010) that can prevent operation if left closed. Reliance to detect this placed on an alarm. Consideration needs to be given to an interlock to prevent reactor start-up if this valve is closed.
			Response: An interlock is provided via the SRPS that prevents reactor start-up unless this manual isolation valve is fully open as stated in Chapter 5, Section 5.5.4.7.1 of the PSAR

Question reference	Section number and name	Topic	ARPANSA Comment, Issue and/or Question and ANSTO's Response
PSA.77.	4.3 Second Shutdown System (SSS)	The SSS will be required in case of a seismic event. The SSS components are all designed as Safety Category 1 items to the SL-2 event. The ball valves and solenoid valves are seen as vulnerable to seismicity.	The duration of the dump (15 s), the sudden gas expansion when the driving gas (helium) enters the Reflector Tank means that the normal operation, expansion and seismic forces need to be superimposed on the reflector tank structure. The seismic potential for a common cause failure of the FSS and SSS caused by the distortion of the Reflector Tank (chimney) should be considered.
			Response: The deflections of the Reflector Vessel arising from the SL-2 seismic event have been analysed and are reported in Chapter 5 of the PSAR. The results show that the vessel and its interconnections are sufficiently robust as to not interfere with the operation of either the FSS or the SSS.

Question reference	Section number and name	Topic	ARPANSA Comment, Issue and/or Question and ANSTO's Response
PSA.78.	4.4 Flap Valves and Siphon Effect Breakers (FV&SEB)	There are several accident sequences where the flap valves and siphon effect breakers are required to actuate. The Flap Valve layout and SEB layout is shown in Fig. 4/18. Five headings have been used to examine the five different safety functions of the FV&SEB).The failure probability estimates are: • For the SEB in the suction line-$1*10^{-3}$. For the S&ISEB in the Reactor and Service Cooling System (RSPCS)-$2.2*10^{-3}$. • For Flap Valves at +6000 Level—and +7000 Level ---$6.5*10^{-6}$ • For Valves at Level 6000 and 7000 (FV6&7) –$6.5*10^{-6}$	The flap valves (FV) and siphon breakers (SEB) are basically passive devices. The key factor may be the flap valve design (see ETRR experience with flap valves), and possible vulnerability to seismic failure. The Flap valves are estimated to be a factor of 100 more reliable than the SEB and this is surprising for such novel features. The value used for individual flap valve failure of $8.7*10^{-5}$ needs justification. Seismic testing of the flap valves is necessary to determine their fragility value for large earthquakes.

Question reference	Section number and name	Topic	ARPANSA Comment, Issue and/or Question and ANSTO's Response
			Response: As pointed out, the SEBs are passive devices. Without readily available data, a very conservative model was adopted, *ie* that human error might render it ineffective. This is not intended to represent a realistic estimate of the failure probability of the SEBs. Refer to Section 4.4.3 of the PSA. The FVs are virtually passive devices, but data for similar devices were available (IAEA TECDOC 478 self operating check valve), and although this is conservative, it does not contain the degree of conservatism of the data used for the SEBs. All Seismic Class 1 items will be seismically qualified.
PSA.79.	4.5 Emergency Water Make Up System (EWMS)	The EWMS is a system designed to provide water to the core chimney in the case that pool water drops to the chimney level. The flooding action is automatic by the opening of two float valves located at the top of the chimney. The success criterion is to compensate for evaporation of water in the chimney due to decay heat. The mean failure probability, based on the Fault Tree Fig 4/25 is $3.4*10^{-3}$	The EWMS is not classed as a Safety Category 1 SSC, yet it is claimed in the PSA for LOCA sequences C1, C2 and C3. There is a single isolation valve that can prevent the EWMS working. Consideration should be given to an interlock, and not just an alarm to prevent reactor power raise if the valve is closed.

Question reference	Section number and name	Topic	ARPANSA Comment, Issue and/or Question and ANSTO's Response
			Response: While in general only Safety category 1 systems were modelled in the PSA, there is no reason why other systems (if relevant) cannot be claimed in the PSA since they assist with accident management. However the EMWS will be required only in the event of a beyond design basis accident. An interlock is provided via the RCMS that prevents reactor start-up unless this manual isolation valve is fully open as stated in Chapter 6, Section 6.7.8.3 of the PSAR.
PSA.80.	4.5 Emergency Water Make Up System (EWMS)—Seismic Considerations.	The EWMS has been designed as a Seismic Category 1 system even though it is designed as a Safety Category 2 SSC. The vulnerable components identified are the float valves	The passive items such as the EWMS tanks and pipe work appear not to have been considered. These may be more vulnerable than other passive items since they are located high in the reactor hall and thus subject to large floor response spectra accelerations.
			Response: Pipework and tanks are to be seismically qualified.
PSA.81.	4.6 Standby Power Supply (SPS)	The SPS is designed to provide electrical power to the reactor under emergency conditions. For the purposes of this PSA the SPS is only needed for the actuation of the SSS, ie 15 seconds after the SRPS initiation.	This SPS requirement is confusing, the SSS (SRPS) is supposed to be fail safe on loss of UPS, so if no UPS the SSS trips. The provision of UPS in this case seems to be aimed at maintaining the UPS to avoid tripping the SSS unless the FSS fails. The logic needs explanation.

Question reference	Section number and name	Topic	ARPANSA Comment, Issue and/or Question and ANSTO's Response
			Response: The SPS is considered in the PSA only in so far as it is needed in the event of loss of electric power (event B2). In the event of the FSS failing, the SSS needs to actuate to shutdown the reactor. If the SPS fails, the SSS will actuate as a fail-safe measure. If the SPS doesn't fail then the SRPS needs to trip the SSS in order that the reactor be shut down.
PSA.82.	4.6 Standby Power Supply (SPS)	For the purposes of this PSA the SPS is only needed for the actuation of the SSS, ie 15 seconds after the SRPS initiation. The mean failure probability is estimated to be $2.2*10^{-3}$.	The SPS success criterion has been discussed in previous questions. In addition there is no apparent consideration of the need to provide electrical power to maintain the mitigation features associated with containment operation and post accident monitoring.
			Response: The operation of the containment function is considered in Chapter 7 of the PSAR. On loss of electric power, the containment function will still be able to be carried out by the SPS. The PAM is described in Chapter 8, Section 8.6 of the PSAR. Please see the response to Question PSA.67.
PSA.83.	4.6 Standby Power Supply (SPS)	Fig 4/26 shows a simplified line diagram of the Standby Power System. In a number of places Automatic Transfer Switches (ATS) are shown that connect the redundant standby systems.	The use of ATSs between the redundant channels would increase operating flexibility, but this is at the expense of independence, separation and redundancy arguments. The use of such ATSs may not satisfy IEEE requirements for keeping safety related electrical systems independent.
			Response: This schematic is incorrect. See PSAR Chapter 9 for the correct schematic, which has a manual transfer arrangement.

Question reference	Section number and name	Topic	ARPANSA Comment, Issue and/or Question and ANSTO's Response
PSA.84.	4.6 Standby Power Supply (SPS)	For the purposes of this PSA the SPS is only needed for the actuation of the SSS, ie 15 seconds after the SRPS initiation.	The way the SPS has been modelled means there has been no PSA evaluation of the reliability of the electrical power supply system. The SPS is a very important safety system since it is part of all Engineered Safety Features (ESF). The reliability of such a system needs to be examined, and should cover maintenance, testing, diesel reliability (start and run), interconnections, control system and seismic design.
			Response: The fail-safe characteristics of the different ESFs, and the fact that no recovery actions are credited in the PSA, make it unnecessary to analyse the reliability of the SPS beyond its performance (UPSs only) for the first 15 seconds of a loss of Mains Power event. In such cases, failure of the UPSs would lead to immediate actuation of the SSS. This modelling approach is appropriate for the purposes of the PSA, which focus on the protection of the public.
PSA.85.	4.6 Standby Power Supply (SPS)	A two redundant system is shown in Fig 4/26.	In view of the fact that only two redundancies are employed there will be a major impact on the Minimum Plant Configuration (MCP). The two would have to be available for operation, within MCP requirements for repair or outage time, and this could be an operational limitation.
			Response: The maintenance requirements will be allowed for in the operational schedule. Class 1E equipment has rigorous maintenance requirements aimed at minimising unplanned down time. The number of DGs would be reassessed if there was any change from Class 1E equipment.

Question reference	Section number and name	Topic	ARPANSA Comment, Issue and/or Question and ANSTO's Response
PSA.86.	5 Event Trees	Provided the reactor is successfully shut down, and the core remains covered with water, natural circulation is sufficient to prevent core damage. If the flap valve actuation fails, the core is assumed to remain in a cooling mode where the decay heat generates some steam bubbles in the core. The bubbles collapse and in the cold water, and cold pool water replenishes the core. This mode of cooling is known as "pulse boiling".	The reference to successful cooling by "pulse boiling" should flap valve actuation fail, requires justification. . Has this mechanism been modelled by the thermal-hydraulic codes used in Ch.16 of the PSAR, and what level of validation and verification is there that the mechanism is effective in removing decay heat.
			Response: "Pulse boiling" has not been modelled by the codes used in the analyses in Chapter 16 of the PSAR as flap valve actuation failure is not assumed there. Pulsed boiling is an effective heat transfer mechanism. It has been observed in a number or reactor experiments (eg. SPERT, CABRI) without any indication that it leads to core damage. See reference "Le calcule termique des reacteurs de recherche refroidie par eaux". S. Fabrega, CEA-R-4114.
PSA.87.	5 Event Trees	No credit is taken for any safety function of the Reactor Control and Monitoring System (RCMS), although it is assumed that the RCMS can initiate inadvertent fault sequences (see A1 and A2 for inadvertent withdrawal of a single control rod)	The RCMS is designed as a Safety Category 1 SSC, although not strictly an ESF. It needs to be examined closely to see the basis for screening out group Control Rod withdrawal scenarios, and failures of interlocks and bypasses.

Question reference	Section number and name	Topic	ARPANSA Comment, Issue and/or Question and ANSTO's Response
			Response: Comment noted. The RCMS is a Safety Category 2 system not 1. Group control rod withdrawal is not a possible event based on the circuit design of the control rod drive mechanism. This is a hardware based interlock not software based. Single control rod movement is only possible based on a frequency based signal being sent to the particular drive mechanism to demand movement The conservative assumption has been made that, while the RCMS can initiate events, it cannot control them. In reality this will not be the case and the RCMS will maintain an adequate Defence In Depth Level 2. Banked CR withdrawal has been ruled out on the basis of independent hardwired devices rendering the likelihood beyond the design basis.
PSA.88.	5.2.1 Erroneous Withdrawal of a Control Rod During Startup—Event A1	The sequence is shown on Event Tree –Fig 5/3 which shows the initiating event and the role of the FRPS, SSS, SRPS and SSS in shutting down the reactor safely. The CDF is estimated as 2.3.1*10^{-11} per year.	The low number for this sequence requires justification. CDF The number also assumes that there is no damage from full power operation if the SSS drops after 15 seconds. If some damage does occur in this timescale, then the CDF increases. The frequency of the event does not appear to have included startup after trips and operation at low power.

Question reference	Section number and name	Topic	ARPANSA Comment, Issue and/or Question and ANSTO's Response
			Response: Full credit was given to the SSS because the analysis in Chapter 16 of the PSAR shows that the SSS would be fully effective (see Section 16.8). The low estimate of CDF, even using conservative data and conservative modelling, is due to the fact that there are inherently safe features and two diverse shutdown systems. The frequency of the initiator A1 will be re-examined, but note that any increase in A1 frequency requires an equal reduction in A2 frequency.
PSA.89.	5.2.1 Erroneous Withdrawal of a Control Rod During Normal Operation—Event A2	The sequence is shown on Event Tree –Fig 5/34which shows the initiating event and the role of the FRPS, SSS, SRPS and SSS in shutting down the reactor safely. The CDF is estimated as $3.47*10^{-10}$ per year.	The low number for this sequence requires justification. See review of section 3.4.3. and the question on the frequency of the initiating event. The number also assumes that there is no damage from full power operation if the SSS is effective after 15 seconds. If some damage does occur in this timescale, then the CDF will increase. . The experience from operating reactors should also be taken into account. From the DIDO PSA the initiating event frequency for an A2 type event was $2.2*10^{-2}$ per year. From HIFAR experience (Table 8.8 of the PSA) a modest reactivity insertion can be expected with a frequency of $3.56*10^{-1}$, which differs from the value here, and should be justified.

Question reference	Section number and name	Topic	ARPANSA Comment, Issue and/or Question and ANSTO's Response
			Response: Full credit was given to the SSS because the analysis in Chapter 16 of the PSAR shows that the SSS would be fully effective (see Section 16.8). The low estimate of CDF, even using conservative data and conservative modelling, is due to the fact that there are inherently safe features and two diverse shutdown systems. Modest reactivity insertions have no effect on this reactor. The comparison is inappropriate. DIDO and HIFAR were designed in the mid 50s, and have no inherent features to prevent fast withdrawal nor bank withdrawal, while the RRR has incorporated the experience accumulated since then and the improvements and refinements of new design methodologies and tools.
PSA.90.	5.2.3 to 5.2.6. Loss of Flow Events B1,B2, B3 and B4	The event tress for these loss of flow sequences are shown in Figs 5/5 to 5/9. Natural circulation is shown as well as the operations of the FSS and SSS in shutting down the reactor. The CDF estimates are: B1-Core Bypass—$3.2*10^{-11}$ per year B2-Loss of Power-$3.7*10^{-9}$ per year B3-Primary Pump Failure—$2.93*10^{-8}$ per year B4-PCS Isolation Valve closure-$8.72*10^{-11}$ per year.	Justification is required that there is no damage from full power operation if on failure of the FSS the SSS is effective after 15 seconds. For B2 it is probably unreasonable to consider fuel damage on failure of FSS and before SSS is effective, since the pumps will coast-down over about 100 seconds. However the frequency to be used for B2 has been raised in previous questions.

Question reference	Section number and name	Topic	ARPANSA Comment, Issue and/or Question and ANSTO's Response
			Response: Full credit was given to the SSS because the analysis in Chapter 16 of the PSAR shows that the SSS would be fully effective. On the frequency of B2 see responses to previous questions.
PSA.91.	5.2.7 Event B5 Fuel Channel Local Blockage	Since it only involves a few channel it is not considered as contributor to CDF and no event tree is derived.	No fuel damage is predicted for this scenario in Ch.16 of the PSAR, since the plates do not exceed 300C. The modelling in Ch.16 needs to be reviewed to ensure no critical thermal hydraulic parameters are exceeded.
			Response: See response to Question PSA.60.
PSA.92.	5.2.8 Event C1--Primary LOCA Caused by a Pipe Rupture Upstream of the Primary Pump	For a rupture in the PCS upstream of the primary pumps the primary pumps draw in air, they cavitate and run outside their operating parameters. The flow in the core is reduced as well as the level in the pool dropping. The leak will continue, until the siphon break becomes effective. The Event tree is shown on Fig 5/9 and includes the FRPS, FSS, SRPS, SSS, SEB,FV and EWMS. The total contribution to CDF is $2.44*10^{-11}$ per year.	The thermal hydraulic modelling of C1 needs careful evaluation, since the pumps would be ineffective once cavitation initiated (no credit for pump coast-down). If the FRPS fails (10^{-3} per demand) then there is a likelihood of an ATWS until the SSS is effective. The frequency of this ATWS is $5.95*10^{-5}*10^{-3}$ or $5.95*10^{-8}$ per year. Do all the assumed core damage sequences for LOCAs correspond to situations where the core is not covered by water.
			Response: Full credit was given to the SSS because the analysis in Chapter 16 of the PSAR shows that the SSS would be fully effective even without pump coast down. See Figure 3/10 in the PSA. Failure of FSS is not an ATWS since the SSS is effective.

Question reference	Section number and name	Topic	ARPANSA Comment, Issue and/or Question and ANSTO's Response
PSA.93.	5.2.9 Event C2. Primary LOCA Caused by A Rupture Downstream of the Primary Pump.	For a pipe rupture in the PCS downstream of the primary pump the pumps are not inhibited from running. The Event Tree is shown in Fig 5/10 and includes the FRPS, FSS, SRPS, SSS, SEB, FV and EWMS. The total contribution to CDF is $1.52*10^{-9}$ per year. If the FSS and SSS are unsuccessful the core is damaged, but provided the SEB works the LOCA is terminated and the core remains covered with water. Natural convection is not possible because all the PCS flap valves are uncovered, however if the reactor is shutdown the core heat could be removed by "pulse boiling".	For both C1 and C2, provided the reactor is shutdown, credit is given to "pulse boiling" as a heat removal mechanism for the decay heat. This claim for successful heat removal was raised in a previous question, is it modelled by the thermal hydraulic codes used in Ch.16 of the PSAR. Are the thermal hydraulic success criteria for flow instability and Departure from Nucleate Boiling (DNBR) relevant in this "pulse boiling " mode. Further justification is needed for the accident behaviour in cases where the reactor is not shutdown.

Question reference	Section number and name	Topic	ARPANSA Comment, Issue and/or Question and ANSTO's Response
			Response: Pulse boiling is an effective cooling method for fuel in a shutdown core provided the core is adequately covered with water. Note that the failure to establish natural convection implies failure to open of four out of four flap valves. Where the core is not shutdown, pulse boiling is assumed to be ineffective. However, the sequences where the reactor is not shutdown are shown to be not credible, having frequencies less than 10^{-9} pa. Modelling of accident behaviour for these sequences is not warranted. Nevertheless, calculations have been performed to design the EMWS. These calculations show that in the incredible case of a LOCA through the beam tubes, the pool water level reaches the upper edge of the chimney approximately 420s after the reactor trip. The maximum heat flux at this time, assuming a power peaking factor of 3, is 8.4 W/cm^2. The heat flux for burn out calculated with the Fabrega correlation[1] is 20 W/cm^2. The DNBR is then 2.5, well above the safety limit for accidental situations (1.5). [1] "Le calcule thermique des reacteurs de recherche refroidis par eau", S. Fabrega, CEA-R-4114.
PSA.94.	5.2.10 Event C3. Reactor Pool Cooling System LOCA.	This event is a rupture of a pipe from the pool cooling system, leading to a LOCA from the reactor pool. The Event Tree is shown in Fig 5/11 and includes the FRPS, FSS, SRPS, SSS, SEB, FV and EWMS. The total contribution to CDF is 1.7*10^{-9} per year.	Further justification is needed for the accident behaviour in cases where the reactor is not shutdown.

Question reference	Section number and name	Topic	ARPANSA Comment, Issue and/or Question and ANSTO's Response
			Response: Core damage is assumed for cases where the reactor does not shutdown in an accident sequence. However, the sequences where the reactor is not shutdown are shown to be not credible, having frequencies less than 10^{-9} pa. The total CDF is shown to be well below regulatory concern. Modelling of accident behaviour for these sequences is not warranted.
PSA.95.	LOCA Events C1, C2 and C3	Same question as above	Do the sequences of core damage from LOCAs end up with no water in the core?
			Response: There are no credible plant damage states with no water in the core (as a result of LOCA or any other initiator).
PSA.96.	5.2.11 Event D Loss of Heat Sink	The Event is a loss of heat extraction capacity by the Secondary Cooling Water (SCS), which prevents power extraction from the PCS. The Event Tree is shown in Fig 5/12 and includes the FRPS, FSS, SRPS, and the SSS. There are four sequences identified that lead to core damage, and the total CDF is estimated as $1.75*10^{-8}$ per year.	This sequence should be reviewed in the light of previous comments on the frequency of loss of power. Whether any core damage occurs depends on the confidence in the thermal hydraulic analysis in Ch.16 of the PSAR. The previous comment about the FRPS reliability should be considered in this context.
			Response: The Frequency of the IE Loss of Mains Power will be re-examined in the FSAR. See also responses to previous comments. Full credit was given to the SSS because the analysis in Chapter 16 of the PSAR shows that the SSS would be fully effective.

Question reference	Section number and name	Topic	ARPANSA Comment, Issue and/or Question and ANSTO's Response
PSA.97.	5.2.12, 5.2.13 and 5.2.14-Events E1, E2 and E3—	Mechanical Damage To Fuel Assemblies In Storage Or Transit. No Event Tree was established for these initiating events since they do not contribute to CDF.	For completeness of the PSA and to permit Level 3 considerations there should be an estimate of the damage frequency and consequences in the PSA.
			Response: See Chapter 7 of the PSA and the response to Question PSA.65.
PSA.98.	5.2.15, 5.2.16,5.2.17, and 5.2.18. Miscellaneous Events—F, G1, G2, and G3.	No Event Tree was established for these initiating events since they do not contribute to CDF.	For completeness of the PSA and to permit Level 3 considerations there should be an estimate of the damage frequency and consequences in the PSA.
			Response: The consequences of events G1, G2 and G3 have been evaluated. Please see Chapter 7 of the PSA and the response to Question PSA.65
PSA.99.	5.3. Event S—Seismic Event	The approach for creating a seismic analysis model involved the development of a seismic Event Tree that linked the seismically induced internal event with the earthquake. The Event Trees are shown on Figs 5/13 to 5/17 and cover the LOCA sequences (equivalent to C1,C2 and C3, and the Loss of Power). No reactivity events were considered to be seismically induced, and loss of flow events would be covered by the loss of power sequences such as B2 and D.	It is not clear what the relative seismic contributions are to LOCA, LOFA, and Loss of Heat Sink CDF estimates. The potential common cause mechanism for failure of the FSS and SSS should be investigated.

Question reference	Section number and name	Topic	ARPANSA Comment, Issue and/or Question and ANSTO's Response
			Response: The relative contributions to the CDF for each of the seismically-induced internal initiating events is indicated in Tables 6/11 to 6/16, and graphically in the Pie-charts 6/2 and 6/3, both for the "up to SL2" level and for the "full hazard curve" level. The contributions indicated correspond to "Loss of Electric Power" (B2) and LOCA events, whilst the consideration of a conditional occurrence probability of 1 for the Loss of Electric Power, makes it irrelevant to consider further events (i.e. Loss of Heat Sink) which are certain to occur on a B2 event. The seismically induced common cause for FSS and SSS has been explicitly included in the Fault Trees for these systems, as Fragility Curves to represent the vulnerability of its components to seismic loads. This is discussed for each system in Section 4 of the PSA

Question reference	Section number and name	Topic	ARPANSA Comment, Issue and/or Question and ANSTO's Response
PSA.100.	6.1 Internal Events Contribution to Core Damage Frequency.	Tables 6/1, 6/2, 6/3, 6/4, 6/5, 6/6, 6,7, 6/8, 6/9, and 6/10 give the sequences that result in CDF and the total CDF contribution for that initiating event. The mean values for each initiating event are shown below: Event Mean CDF Contribution A1 $2.32*10^{-11}$ per year A2 $3.48*10^{-10}$ per year B1 $3.23*10^{-11}$ per year B2 $4.88*10^{-09}$ per year B3 $2.96*10^{-08}$ per year B4 $1.19*10^{-10}$ per year C1 $2.51*10^{-10}$ per year C2 $1.28*10^{-09}$ per year C3 $1.07*10^{-09}$ per year D $1.75*10^{-08}$ per year Total $6.96*10^{-08}$ per year	These estimates should be reviewed in the light of the previous comments.
			Response: As mentioned previously, the frequencies of IEs B2 and A1 will be re-examined in the FSAR Stage. It is not expected to significantly affect the estimated CDF.

Question reference	Section number and name	Topic	ARPANSA Comment, Issue and/or Question and ANSTO's Response
PSA.101.	6.1 Internal Events Contribution to Core Damage Frequency.	Tables 6/1, 6/2, 6/3, 6/4, 6/5, 6/6, 6,7, 6/8, 6/9, and 6/10 give the sequences that result in CDF and the total CDF contribution for that initiating event. The mean values for each initiating event are shown below: Event Mean CDF Contribution A1 $2.32*10^{-11}$ per year A2 $3.48*10^{-10}$ per year B1 $3.23*10^{-11}$ per year B2 $4.88*10^{-09}$ per year B3 $2.96*10^{-08}$ per year B4 $1.19*10^{-10}$ per year C1 $2.51*10^{-10}$ per year C2 $1.28*10^{-09}$ per year C3 $1.07*10^{-09}$ per year D $1.75*10^{-08}$ per year Total $6.96*10^{-08}$ per year	The review has commented on the need to give additional consideration to core safety in the period between failure of the FSS (which is dominated by the FRPS failure rate of 10^{-3} per demand) and success of the SSS. The estimates should be reviewed in this context. The importance of the loss of power sequences (B2 and D) is evident. They make the major contribution to this pre-SSS success accident mode. Whether there is any fuel damage is a matter of importance.
			Response: Full credit was given to the SSS because the analysis in Chapter 16 of the PSAR shows that the SSS would be fully effective in all PIEs. The frequencies of IEs B2 and A1 will be re-examined in the FSAR according to previous comments on the estimation of their frequency. It is not expected to significantly affect the estimated CDF.

Question reference	Section number and name	Topic	ARPANSA Comment, Issue and/or Question and ANSTO's Response
PSA.102.	6.1 Internal Events Contribution to Core Damage Frequency.	Tables 6/1, 6/2, 6/3, 6/4, 6/5, 6/6, 6,7, 6/8, 6/9, and 6/10 give the sequences that result in CDF and the total CDF contribution for that initiating event. The mean values for each initiating event are shown below: Event Mean CDF Contribution A1 $2.32*10^{-11}$ per year A2 $3.48*10^{-10}$ per year B1 $3.23*10^{-11}$ per year B2 $4.88*10^{-09}$ per year B3 $2.96*10^{-08}$ per year B4 $1.19*10^{-10}$ per year C1 $2.51*10^{-10}$ per year C2 $1.28*10^{-09}$ per year C3 $1.07*10^{-09}$ per year D $1.75*10^{-08}$ per year Total $6.96*10^{-08}$ per year	Justification is required for the lack of treatment of the LOCA sequences in the off-site release analysis. CDF.
			Response: The total CDF (including LOCA events, internal and external causes) is below regulatory criteria (*ie* below the most stringent frequency associated with the safety objective in the Regulatory Assessment Principles). It is therefore not necessary to determine consequences as shown in the RAPs.

Question reference	Section number and name	Topic	ARPANSA Comment, Issue and/or Question and ANSTO's Response
PSA.103.	6.2 Seismic Event Contribution to Core Damage Frequency	The seismic contribution has been analysed in two different scenarios, namely events up to the SL-2 (10,,000 year return period), and all seismic events indicated in Hazard Curve Fig 3/21. The mean CDF results for the LOCA sequences and Loss of Power are shown below: Event up to SL-2 All C3 $3.18*10^{-11}$ $2.08*10^{-08}$ C1 $1.55*10^{-11}$ $1.67*10^{-08}$ C2 $2.08*10^{-11}$ $1.73*10^{-08}$ B2 $2.04*10^{-10}$ $1.71*10^{-08}$ Total $1.91*10^{-10}$ $7.91*10^{-08}$	For the full range of earthquakes it is not clear why numbers of the order 10^{-8} are estimated. More information is required on the derivation of this value and the reliability of safety systems following a seismic event. It is not clear if the loss of power includes the loss of heat sink (D), which is a significant internal initiating event contributor. Is it included as part of B2.

Question reference	Section number and name	Topic	ARPANSA Comment, Issue and/or Question and ANSTO's Response
			Response: For items identified as seismically vulnerable for PSA purposes, the HCPLF corresponds to 0.3 g ground motion and the median fragility to 0.8 g. The 100,000 year return period PGA is 0.745 at which the probability of failure is <0.5. The FVs, SEBs etc were not considered seismically vulnerable because they are robust passive devices and if they were to fail, their most likely failure mode would be to break the siphon. Whilst the LOCA conditional probability at this extreme seismic event would approach unity because of the numerous pipe sections (each with a probability of just under 0.5), the many safety systems, some of which have no seismically vulnerable components, leads to a low CDF of around 10^3 times lower than the seismic initiator.

Question reference	Section number and name	Topic	ARPANSA Comment, Issue and/or Question and ANSTO's Response
PSA.104.	6.4 Importance Factors	The Fussell-Vesely Risk Reduction and Risk Increase values were obtained and are shown in Table 6/16. The first 5 most important are shown below: Event Name Importance FRPS 0.883 E-PP-2 0.264 E-PP-1 0.264 SRPS 0.229 E-SSS-1-6A 0.18 These are in order: Failure of the First Reactor Protection System (FRPS) Failure of the PCS pumps (E-PP-1 and –2) Failure of the Second Reactor Protection System (SRPS) Failure SS Dump Valves to open (E-SSS-1-6A)	The failure of the pumps should be re-examined in the light of the discussion of the loss of off-site power number.

Question reference	Section number and name	Topic	ARPANSA Comment, Issue and/or Question and ANSTO's Response
			Response: As stated above, the frequencies of IEs B2 and A1 will be re-examined in the FSAR according to previous comments on the estimation of their frequency. It is not expected to significantly affect the estimated CDF. CDF and event importance values will be recomputed. As pointed out, the importance of the PCS pump failure may be affected.
PSA.105.	7.1 Level 3 Considerations and Comparison with Objectives	The mean values of CDF determined in Ch.6, both from internal events and seismically induced events were low. A reason for these low levels was the parallel design activity with the PSA which designed out weak points. The associated risk values are well within the Regulatory Assessment Principles as shown on Fig 7/3. The 95% confidence of the CDF also lies within the Safety Objective curve shown on Fig. 7/3.	The low values determined in Ch.6 have been discussed above (see the range of comments on 6.1). The revised values however would not change the conclusion that the CDF values and comparison with Fig. 7.3 are satisfactory. However, there is a need to treat the LOCAs and non LOCA events separately, since the subsequent release characteristics are different.
			Response: As stated above, the frequencies of IEs B2 and A1 will be re-examined in the FSAR according to previous comments on the estimation of their frequency. It is not expected to significantly affect the estimated CDF. CDF and event importance values will be recomputed. No consequence calculation is needed for plant damage states that have frequency below regulatory criteria.

Question reference	Section number and name	Topic	ARPANSA Comment, Issue and/or Question and ANSTO's Response
PSA.106.	7.4 Dose Estimations	Several dose estimations were carried out for the reactor facility using the PC COSYMA code. The release assumptions are the same as used for the Siting Reference Accident, and gives credit to the retention of fission products in the pool. The Reference accident case consider 25% of the core melted under the water and resulted in a dose of 0.21 mSv to a person at boundary of the exclusion zone of 1600 m.	There appears to be no treatment of the LOCA sequences for off-site releases. This should be justified.
			Response: No consequence calculation is needed for plant damage states that have frequency below regulatory criteria.
PSA.107.	7.5 Risk Results and Comparison with Regulatory Assessment Principles.	In Fig 7/3 the CDF is shown without dose estimation, but showing that is below the most stringent frequency for the safety objective. It is stated that the expected risk contribution of the selected accidents is well below the acceptable levels. It also states that that the maximum doses do not require any off-site emergency measures. If aircraft crash and strike by military shell included the total core damage frequency increases to $3.7 * 10^{-7}$ per year.	The previous question on LOCA sequences also applies here. For the case of aircraft crash and military shell it is not clear what the impact would be on core cooling
			Response: No consequence calculation is needed for plant damage states that have frequency below regulatory criteria.

Question reference	Section number and name	Topic	ARPANSA Comment, Issue and/or Question and ANSTO's Response
PSA.108.	7.3 Containment Response	The containment has been designed to contain any radioactive release to the environment. It has been designed with dual closures for systems open to the atmosphere within the containment. It will, in general, automatically seal on the detection of high activity in the ventilation stack. A containment energy removal system has been designed to keep the containment within its specified pressure under design basis accidents. In addition a containment pressure relief system is provided to prevent damage to the containment structure. The Containment Isolation System (CIS) is fail safe on loss of power, but the energy removal system requires stand-by power.	The containment function has not been considered for the range of event trees in the PSA since the concentration was on the CDF, which is not affected by the containment function. However, the containment function is an important part of any PSA Level 3 consideration. Its availability and performance under the range of internal and external events described in this PSA should be considered.

Question reference	Section number and name	Topic	ARPANSA Comment, Issue and/or Question and ANSTO's Response
			Response: The PSA concentrated upon the determination of the likelihood of release of radioactive material. The determination of consequences for the selected fault sequences was carried out in a very conservative manner. The results show that the risks associated with the operation of the RRR are very low. For design basis internal and external events, the containment was conservatively modelled as functioning at its design basis level. The conservatism was carried over into the analysis of those fault sequences that led to the release of radioactive material. (These would normally have been considered in a best estimate manner.) Considerations of failure of the containment are not considered to change the residual risk of the plant.
PSA.109.	7.2.2 Irradiated Fuel Handling Events—E2 to E3	These events have been considered separately since not CDF contributors. Only mechanical damage is considered in the pools or in transit. Event E3, associated with transit is the bounding case for these events. It is estimated to have a frequency of $3 * 10^{-3}$ per year, and a release of $6.25 * 10^{-4}$ of the core inventory of fission products. It is plotted on Fig.7/3.	The estimate for the frequency of mechanical damage to a fuel element should be justified. In the case of the HIFAR fuel elements have been dropped on three occasions (without any release). It should be anticipated that fuel elements will be dropped more than once in the life of the RRR. However, as shown in the Dose Estimations (7.4) the dose is small (0.53 micro Sv)
			Response: The frequency to be estimated is that of mechanical damage to a fuel element WITH release. The one cited case is the only one identified where a release was reported. Both the frequency and consequence were conservatively increased from the data derived from the incident.

Question reference	Section number and name	Topic	ARPANSA Comment, Issue and/or Question and ANSTO's Response
PSA.110.	7.2.3 Heavy Water Leak Events--F	The potential spill of heavy water outside the reactor pool is considered unlikely any release would effect the operators, but no significant release to the atmosphere is expected.	The leakage of tritium to the atmosphere should be less than HIFAR for normal operation. A gross spill however should be anticipated (pipe break at about 10^{-4} per year), or more likely due to a maintenance error (say 5* 10^{-2} per year). A spill of 100 litres is not unexpected, but the consequences off site would be trivial.
			Response: The intention of this PSA (inter alia) was to identify possible design improvements through the design process, understand the plant and demonstrate compliance with the regulatory assessment principles. Since the consequences off-site would be negligible, this event was not analysed further.
PSA.111.	7.2.4 Reactor Utilisation Events	The basic event for the PSA evaluations consists of the loss of cooling flow (either local or global) to the bulk production irradiation facility targets. The annual frequency of a local blockage (G1) is estimated as $1.2*10^{-5}$ per year.	This estimate for the likelihood of this event should be justified, since it is based on estimates for maintenance error (M) and its detection, discussed previously. Such errors have occurred in research reactors and the frequency should be based on an analysis of pool reactor operational experience. The estimate of the off-site dose (5.64 micro-Sv) is low.
			Response: The estimate is based on two independent operator errors; that of the person carrying out maintenance tasks and that of the supervisor in checking afterwards. It is worth noting that IAEA TECDOC 478 quotes a figure for plugging of small diameter pipes of 0.9 x 10^{-5} per year. Moreover, the estimated dose associated to this event is so low, that even considering a sufficiently broad uncertaintly in its frequency, it does not pose a significant risk on the public.

Question reference	Section number and name	Topic	ARPANSA Comment, Issue and/or Question and ANSTO's Response
PSA.112.	7.2.4 Reactor Utilisation Events-G2	The global loss of RSPCS flow may be initiated by a failure in the cooling system. This trips the reactor—(FRPS and FSS) and power generation is limited to decay heat. The sequence is shown in the Fault Tree (Fig7/1). It includes pump failure, maintenance error, or valve failure and is estimated as $2.8*10^{-3}$ per year. The FRPS failure is estimated as 10^{-3} per year to give a postulated event frequency (without trip action) of $2.8*10^{-6}$ per year	The loss of mains power can be anticipated at about twice per year. If the FRPS fails to trip the reactor then the event frequency (without trip until SSS action) is about $2*10^{-3}$ per year. The consequences are estimated to be 67.7 micro-Sv, which is just below the Safety Objective (Fig.7.3)
			Response: Consideration of the frequency of loss of offsite power is contained in the response to Question PSA.57. Loss of offsite power will *per se* de-energise the electromagnets holding up the control rods, open the pneumatic system valves and lead to shutdown of the reactor. In the unlikely event that the rods do not fall into the core, the SRPS will trip and shut down the reactor. The likelihood of failure of the FRPS must therefore be considered in conjunction with failure of the FSS. It cannot be considered by itself. Loss of offsite power is treated as an initiator in its own right. It should not be double counted as an initiator for a global loss of RSPCS flow

Question reference	Section number and name	Topic	ARPANSA Comment, Issue and/or Question and ANSTO's Response
PSA.113.	7.2.4 Reactor Utilisation Events-G3	The maximum uranium metal foil movement is expected to be 344 rigs per year. The event considered is an early transfer of the rig to the hot cell and melting of the target in the hot cell. The estimated frequency of such an error is given in Table 7/1 as $6.9*10^{-5}$ per year.	This estimate for the likelihood of this event should be justified, since it is based on low estimates for operator error (M) and its detection. The number of movements per year is quite significant, and the ability of the radiation detector to detect a can that has decayed for an insufficient period of time should be justified. Target transfer errors have occurred in research reactors and the frequency should take account of pool reactor operational experience. The estimate of the off-site dose (12.7micro-Sv) is low.
			Response: Considerable thought has been expended on the interlock for this event. The detectors are duplicated and the whole system is classified as Safety Category 1 and compliant with applicable IEEE Cat 1 standards. The radiation levels for various targets have been analysed. The differential between an insufficiently cooled Mo99 target and others is large. Nevetheless an excess radiation from another target would prevent removal and hence the interlock would err on the side of safety. Operational experience at other research reactors will be taken into account in the preparation of the FSAR.

Appendix PSA.1

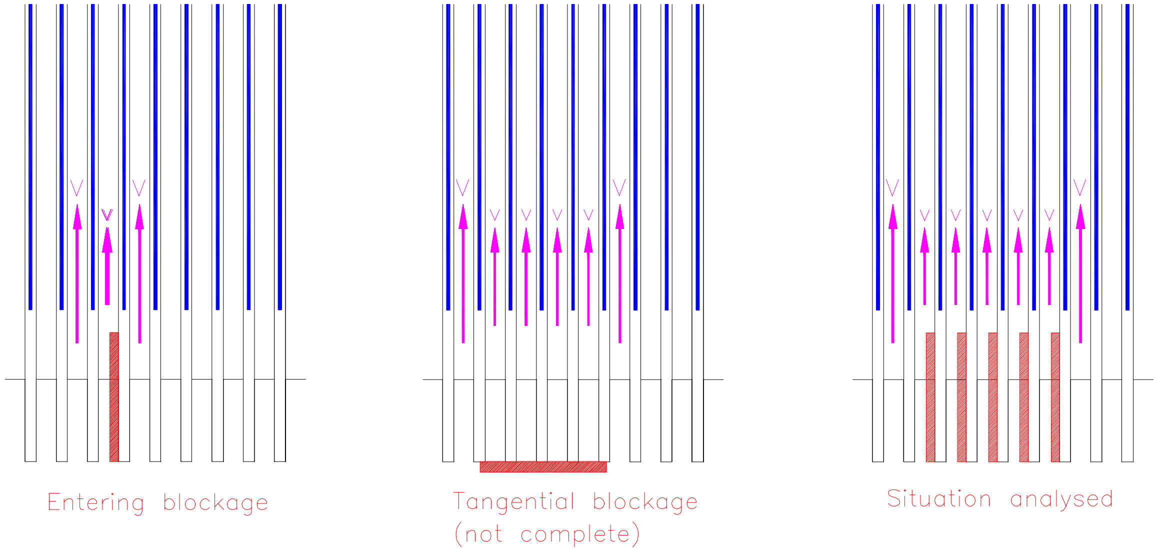

Figure PSA.60.1: Case analysed for the partial blockage of a cooling channel

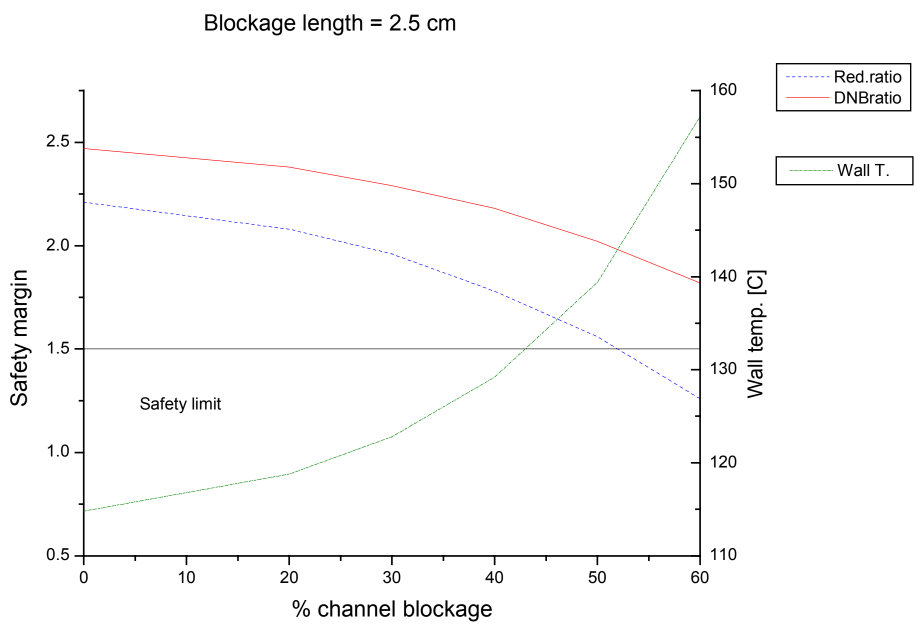

Figure PSA.60.2: Margin to critical Phenomena for partial blockage of cooling channels (Case 1)

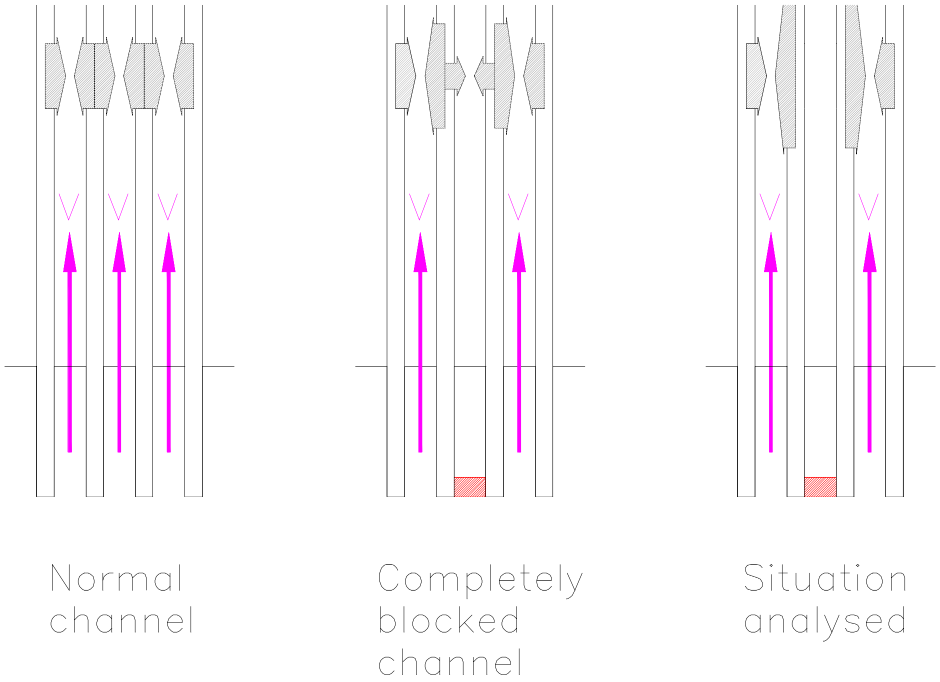

Figure PSA.60.3: Total Blockage of a cooling channel (Case 2)